EUROPEAN PARLIAMENT

SCIENTIFIC AND TECHNOLOGICAL OPTIONS ASSESSMENT

STOA

DEVELOPMENT OF SURVEILLANCE TECHNOLOGY AND RISK OF ABUSE OF ECONOMIC INFORMATION

(an appraisal of technologies for political control)

Part 4/4

The state of the art in Communications Intelligence(COMINT)of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems, and its applicability to COMINT targeting and selection, including speech recognition

---

Working document for the STOA Panel

Luxembourg, April 1999   PE 168.184/Part3/4

Directorate General for Research

| DA | DE | EL | EN | ES | FR | IT | NL | PT | FI | SV |

Further information or other reports on the same topic may be obtained from the European Parliament, Luxembourg http://www.europarl.eu.int/dg4/stoa/en The author's home page is at http://www.gn.apc.org/duncan If you are posting links to others, please link to this page

Interception Capabilities2000

Contents

1. Organisations and methods

2. Intercepting internationalcommunications

ILC communications collection

Access

Operation SHAMROCK

High frequency radio interception

Space interception of inter-city networks

Sigint satellites

COMSAT ILC collection

Submarine cable interception

Intercepting the Internet

Covert collection of high capacity signals

New satellite networks

3. ECHELON and Comint production

The "Watch List"

New information about ECHELON sites and systems

Westminster, London : Dictionary computer

Sugar Grove, Virginia : COMSAT interceptionat ECHELON site

Sabana Seca, Puerto Rico and Leitrim, Canada: COMSAT interception sites

Waihopai, New Zealand : Intelsat interceptionat ECHELON site

ILC processing techniques

4. Comint and Law Enforcement

Misrepresentation of law enforcement interceptionrequirements

Law enforcement communications interception- policy development in Europe

5. Comint and economic intelligence

Tasking economic intelligence

Disseminating economic intelligence

The use of Comint economic intelligenceproduct

Panavia European Fighter Aircraft consortiumand Saudi Arabia

Thomson CSF and Brazil

Airbus Industrie and Saudi Arabia

International trade negotiations

Targeting host nations

6. Comint capabilities after2000

Developments in technology

Policy issues for the European Parliament

Technical annexe

Broadband (high capacity multi-channel)communications

Communications intelligence equipment

Wideband extraction and signal analysis

Filtering, data processing, and facsimile analysis

Traffic analysis, keyword recognition, textretrieval, and topic analysis

Speech recognition systems

Continuous speech recognition

Speaker identification and other voice messageselection techniques

"Workfactor reduction"; the subversion of cryptographicsystems

Glossary and definitions

Footnotes

Summary

1. **Communications intelligence**(Comint) involving the covert interception of foreign communications hasbeen practised by almost every advanced nation since international telecommunicationsbecame available. Comint is a large-scale industrial activity providingconsumers with intelligence on diplomatic, economic and scientific developments.The capabilities of and constraints on Comint activity may usefully beconsidered in the framework of the "intelligence cycle" (section 1).

2. Globally, about 15-20 billion Eurois expended annually on Comint and related activities. The largest componentof this expenditure is incurred by the major English-speaking nations ofthe UKUSA alliance.**(1)**This report describes how Comint organisations have for more than 80 yearsmade arrangements to obtain access to much of the world's internationalcommunications. These include the unauthorised interception of commercialsatellites, of long distance communications from space, of undersea cablesusing submarines, and of the Internet. In excess of 120 satellite systemsare currently in simultaneous operation collecting intelligence (section2).

3. The highly automated UKUSA systemfor processing Comint, often known as ECHELON, has been widely discussedwithin Europe following a 1997 STOA report.**(2)**That report summarised information from the only two primary sources thenavailable on ECHELON.**(3)**This report provides original new documentary and other evidence aboutthe ECHELON system and its involvement in the interception of communicationsatellites (section 3). A technical annexe give a supplementary, detaileddescription of Comint processing methods.

4. Comint information derived fromthe interception of international communications has long been routinelyused to obtain sensitive data concerning individuals, governments, tradeand international organisations. This report sets out the organisationaland reporting frameworks within which economically sensitive informationis collected and disseminated, summarising examples where European commercialorganisations have been the subject of surveillance (section 4).

5. This report identifies a previouslyunknown international organisation - "ILETS" - which has, without parliamentaryor public discussion or awareness, put in place contentious plans to requiremanufacturers and operators of new communications systems to build in monitoringcapacity for use by national security or law enforcement organisations(section 5).

6. Comint organisations now perceivethat the technical difficulties of collecting communications are increasing,and that future production may be costlier and more limited than at present.The perception of such difficulties may provide a useful basis for policyoptions aimed at protective measures concerning economic information andeffective encryption (section 6).

7. **Key findings** concerning thestate of the art in Comint include :

- Comprehensive systems exist to access,intercept and process every important modern form of communications, withfew exceptions (section 2, technical annexe);
- Contrary to reports in the press, effective"word spotting" search systems automatically to select telephone callsof intelligence interest are not yet available, despite 30 years of research.However, speaker recognition systems - in effect, "voiceprints" - havebeen developed and are deployed to recognise the speech of targeted individualsmaking international telephone calls;

- Recent diplomatic initiatives by the UnitedStates government seeking European agreement to the "key escrow" systemof cryptography masked intelligence collection requirements, and formedpart of a long-term program which has undermined and continues to underminethe communications privacy of non-US nationals, including European governments,companies and citizens;

- There is wide-ranging evidence indicatingthat major governments are routinely utilising communications intelligenceto provide commercial advantage to companies and trade.

1. Organisations and methods

What is communications intelligence?

1. Communications intelligence (Comint)is defined by NSA, the largest agency conducting such operations as "technicaland intelligence information derived from foreign communications by otherthan their intended recipient". (4)Comintis a major component of Sigint (signals intelligence), which also includesthe collection of non-communications signals, such as radar emissions.(5)Although this report deals with agencies and systems whose overall taskmay be Sigint, it is concerned only with Comint.

2. Comint has shadowed the developmentof extensive high capacity new civil telecommunications systems, and hasin consequence become a large-scale industrial activity employing manyskilled workers and utilising exceptionally high degrees of automation.

3. The targets of Comint operationsare varied. The most traditional Comint targets are military messages anddiplomatic communications between national capitals and missions abroad.Since the 1960s, following the growth of world trade, the collection ofeconomic intelligence and information about scientific and technical developmentshas been an increasingly important aspect of Comint. More recent targetsinclude narcotics trafficking, money laundering, terrorism and organisedcrime.

4. Whenever access to internationalcommunications channels is obtained for one purpose, access to every othertype of communications carried on the same channels is automatic, subjectonly to the tasking requirements of agencies. Thus, for example, NSA andits British counterpart GCHQ, used Comint collected primarily for otherpurposes to provide data about domestic political opposition figures inthe United States between 1967 and 1975.

UKUSAalliance

5. The United States SigintSystem (USSS) consists of the National Security Agency (NSA), militarysupport units collectively called the Central Security Service, and partsof the CIA and other organisations. Following wartime collaboration, in1947 the UK and the US made a secret agreement to continue to conduct collaborativeglobal Comint activities. Three other English-speaking nations, Canada,Australia and New Zealand joined the UKUSA agreement as "Second Parties".The UKUSA agreement was not acknowledged publicly until March 1999, whenthe Australian government confirmed that its Sigint organisation, DefenceSignals Directorate (DSD) "does co-operate with counterpart signals intelligenceorganisations overseas under the UKUSA relationship".(6)The UKUSA agreement shares facilities, tasks and product between participatinggovernments.

6. Although UKUSA Comint agency staffsand budgets have shrunk following the end of the cold war, they have reaffirmedtheir requirements for access to all the world's communications. AddressingNSA staff on his departure in 1992, then NSA director Admiral William Studemandescribed how "the demands for increased global access are growing". The"business area" of "global access" was, he said, one of "two, hopefullystrong, legs upon which NSA must stand" in the next century.(7)

OtherComint organisations

7. Besides UKUSA, there at least30 other nations operating major Comint organisations. The largest is theRussian FAPSI, with 54,000 employees.(8)China maintains a substantial Sigint system, two stations of which aredirected at Russia and operate in collaboration with the United States.Most Middle Eastern and Asian nations have invested substantially in Sigint,in particular Israel, India and Pakistan.
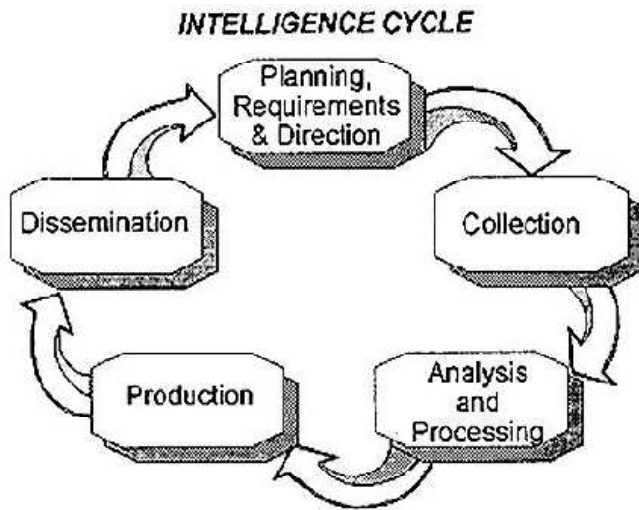
How intelligence works

8. In the post cold war era, Comint interceptionhas been constrained by recognisable industrial features, including therequirement to match budgets and capabilities to customer requirements.The multi-step process by means of which communications intelligence issought, collected, processed and passed on is similar for all countries,and is often described as the "intelligence cycle". The steps of the intelligencecycle correspond to distinct organisational and technical features of Comintproduction. Thus, for example, the administration of NSA's largest fieldstation in the world, at Menwith Hill in England and responsible for operatingover 250 classified projects, is divided into three directorates: OP, Operationsand Plans; CP, Collection Processing; and EP, Exploitation and Production.

Planning

9. Planning first involves determiningcustomer requirements. Customers include the major ministries of the sponsoringgovernment - notably those concerned with defence, foreign affairs, security,trade and home affairs. The overall management of Comint involves the identificationof requirements for data as well as translating requirements into potentiallyachievable tasks, prioritising, arranging analysis and reporting, and monitoringthe quality of Comint product.

10. Once targets have beenselected, specific existing or new collection capabilities may be tasked,based on the type of information required, the susceptibility of the targetedactivity to collection, and the likely effectiveness of collection.

Accessand collection

INTELLIGENCE CYCLE

Planning, Requirements & Direction

Collection

Dissemination

Analysis and Processing

Production

essential of Comint is access to the desired communications medium so that communications may be intercepted. Historically, where long-range radio communications were used, this task was simple. Some important modern communications systems are not "Comint friendly" and may require unusual, expensive or intrusive methods to gain access. The physical means of communication is usually independent of the type of information carried. For example, inter-city microwave radio-relay systems, international satellite links and fibreoptic submarine cables will all usually carry mixed traffic of television, telephone, fax, data links, private voice, video and data.

12. Collection follows interception, but is a distinct activity in that many types of signals may be intercepted but will receive no further processing save perhaps technical searches to verify that communications patterns remain unchanged. For example, a satellite interception station tasked to study a newly launched communications satellite will set up an antenna to intercept all that the satellite sends to the ground. Once a survey has established which parts of the satellite's signals carry, say, television or communications of no interest, these signals will not progress further within the system.

13. Collection includes both acquiring information by interception and passing information of interest downstream for processing and production. Because of the high information rates used in many modern networks, and the complexity of the signals within them, it is now common for high speed recorders or "snapshot" memories temporarily to hold large quantities of data while processing takes place. Modern collection activities use secure, rapid communications to pass data via global networks to human analysts who may be a continent away. Selecting messages for collection and processing is in most cases automated, involving large on-line databanks holding information about targets of interest.

Processing

14. Processing is the conversion of collected information into a form suitable for analysis or the production of intelligence, either automatically or under human supervision. Incoming communications are normally converted into standard formats identifying their technical characteristics, together with message (or signal) related information (such as the telephone numbers of the parties to a telephone conversation).

15. At an early stage, if it is not inherent in the selection of the message or conversation, each intercepted signal or channel will be described in standard "case notation". Case notation first identifies the countries whose communications have been intercepted, usually by two letters. A third letter designates the general class of communications: C for commercial carrier intercepts, D for diplomatic messages, P for police channels, etc. A fourth letter designates the type of communications system (such as S for multi-channel). Numbers then designate particular links or networks. Thus for example, during the 1980s NSA intercepted and processed traffic designated as "FRD" (French diplomatic) from Chicksands, England, while the British Comint agency GCHQ deciphered "ITD" (Italian diplomatic) messages at its Cheltenham headquarters. (9)

16. Processing may also involve translation or "gisting" (replacing a verbatim text with the sense or main points of a communication). Translation and gisting can to some degree be automated.

Production and dissemination

17. Comint production involves analysis, evaluation, translation and interpretation of raw data into finished intelligence. The final step of the intelligence cycle is dissemination, meaning the passing of reports to the intelligence consumers. Such reports can consist of raw (but decrypted and/or translated) messages, gists, commentary, or extensive analyses. The quality and relevance of the disseminated reports lead in turn to the re-specification of intelligence collection priorities, thereby completing the intelligence cycle.

18. The nature of dissemination is highly significant to questions of how Comint is exploited to obtain economic advantage. Comint activities everywhere are highly classified because, it is argued, knowledge of the success of interception would be likely to lead targets to change their communications methods to defeat future interception. Within the UKUSA system, the dissemination of Comint reports is limited to individuals holding high-level security "SCI" clearances.(10) Further, because only cleared officials can see Comint reports, only they can set requirements and thus control tasking. Officials of commercial companies normally neither have clearance nor routine access to

Comint, and may therefore only benefit from commercially relevant Comint information to the extent

Comint,and may therefore only benefit from commercially relevant Comint informationto the extent that senior, cleared government officials permit. The waysin which this takes place is described in Section 5, below.

19. Dissemination is further restrictedwithin the UKUSA organisation by national and international rules generallystipulating that the Sigint agencies of each nation may not normally collector (if inadvertently collected) record or disseminate information aboutcitizens of, or companies registered in, any other UKUSA nation. Citizensand companies are collectively known as "legal persons". The opposite procedureis followed if the person concerned has been targeted by their nationalComint organisation.

20. For example, Hager has described(11)how New Zealand officials were instructed to remove the names of identifiableUKUSA citizens or companies from their reports, inserting instead wordssuch as "a Canadian citizen" or "a US company". British Comint staff havedescribed following similar procedures in respect of US citizens followingthe introduction of legislation to limit NSA's domestic intelligence activitiesin 1978.(12)The Australian government says that "DSD and its counterparts operate internalprocedures to satisfy themselves that their national interests and policiesare respected by the others ... the Rules [on Sigint and Australian persons]prohibit the dissemination of information relating to Australian personsgained accidentally during the course of routine collection of foreigncommunications; or the reporting or recording of the names of Australianpersons mentioned in foreign communications".(13)The corollary is also true; UKUSA nations place no restrictions on intelligencegathering affecting either citizens or companies of any non-UKUSA nation,including member states of the European Union (except the UK).

2.Intercepting international communications

International Leased Carrier(ILC) communications

21. It is a matter of record that foreigncommunications to and from, or passing through the United Kingdom and theUnited States have been intercepted for more than 80 years.(14)Then and since, most international communications links have been operatedby international carriers, who are usually individual national PTTs orprivate companies. In either case, capacity on the communication systemis leased to individual national or international telecommunications undertakings.For this reason, Comint organisations use the term ILC (International LeasedCarrier) to describe such collection.

Highfrequency radio

22. Save for direct landlineconnections between geographically contiguous nations, high frequency (HF)radio system were the most common means of international telecommunicationsprior to 1960, and were in use for ILC, diplomatic and military purposes.An important characteristic of HF radio signals is that they are reflectedfrom the ionosphere and from the earth's surface, providing ranges of thousandsof miles. This enables both reception and interception.

Microwaveradio relay

23. Microwave radio was introducedin the 1950s to provide high capacity inter-city communications for telephony,telegraphy and, later, television. Microwave radio relay communicationsutilise low power transmitters and parabolic dish antennae placed on towersin high positions such as on hilltops or tall buildings. The antennae areusually 1-3m in diameter. Because of the curvature of the earth, relaystations are generally required every 30-50km.

Subseacables

24. Submarine telephone cablesprovided the first major reliable high capacity international communicationssystems. Early systems were limited to a few hundred simultaneous telephonechannels. The most modern optical fibre systems carry up to 5 Gbps (Gigabitsper second) of digital information. This is broadly equivalent to about60,000 simultaneous telephone channels.

Communicationssatellites

25. Microwave radio signalsare not reflected from the ionosphere and pass directly into space. Thisproperty has been exploited both to provide global communications and,conversely, to intercept such communications in space and on land. Thelargest constellation of communications satellites (COMSATs) is operatedby the International Telecommunications Satellite organisation (Intelsat),an international treaty organisation. To provide permanent communicationsfrom point to point or for broadcasting purposes, communications satellitesare placed into so-called "geostationary" orbits such that, to the earth-basedobserver, they appear to maintain the same position in the sky.

26. The first geostationaryIntelsat satellites were orbited in 1967. Satellite technology developedrapidly. The fourth generation of Intelsat satellites, introduced in 1971,provided capacity for 4,000 simulataneous telephone channels and were capableof handling all forms of communications simultaneously -telephone, telex,telegraph, television, data and facsimile. In 1999, Intelsat operated 19satellites of its 5th to 8th generations. The latest generationcan handle the equivalent to 90,000 simultaneous calls.

Communicationstechniques

27. Prior to 1970, most communicationssystems (however carried) utilised analogue or continuous wave techniques.Since 1990, almost all communications have been digital, and are providingever higher capacity. The highest capacity systems in general use for theInternet, called STM-1 or OC-3, operates at a data rate of 155Mbs. (Millionbits per second; a rate of 155 Mbps is equivalent to sending 3 millionwords every second, roughly the text of one thousand books a minute.) Forexample, links at this capacity are used to provide backbone Internet connectionsbetween Europe and the United States. Further details of communicationstechniques are given in the technical annexe.

ILC communicationscollection

Access

28. Comint collection cannottake place unless the collecting agency obtains access to the communicationschannels they wish to examine. Information about the means used to gainaccess are, like data about code-breaking methods, the most highly protectedinformation within any Comint organisation. Access is gained both withand without the complicity or co-operation of network operators.

OperationSHAMROCK

29. From 1945 onwards in theUnited States the NSA and predecessor agencies systematically obtainedcable traffic from the offices of the major cable companies. This activitywas codenamed SHAMROCK. These activities remained unknown for 30 years,until enquiries were prompted by the Watergate affair. On 8 August 1975,NSA Director Lt General Lew Allen admitted to the Pike Committee of theUS House of Representatives that :
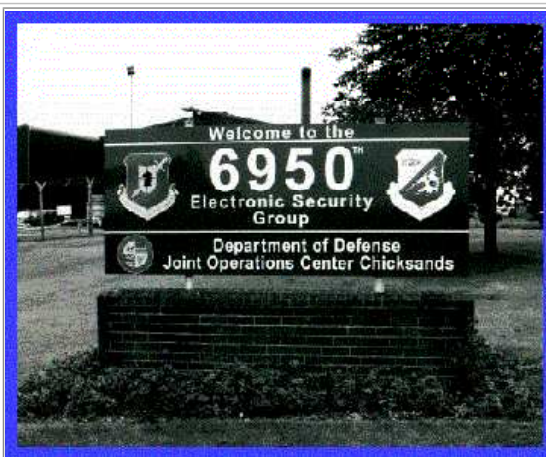
> "NSA systematicallyintercepts international communications, both voice and cable".

30. He also admitted that "messagesto and from American citizens have been picked up in the course of gatheringforeign intelligence". US legislators considered that such operations mighthave been unconstitutional. During 1976, a Department of Justice team investigatedpossible criminal offences by NSA. Part of their report was released in1980. It described how intelligence on US citizens:

> "was obtained incidentally inthe course of NSA's interception of aural and non-aural (e.g., telex) internationalcommunications and the receipt of GCHQ-acquired telex and ILC (InternationalLeased Carrier) cable traffic (SHAMROCK)" (emphasis in original).(15)

| High frequency radio interceptionantenna (AN/FLR9) | DODJOCC sign at NSA station,Chicksands |

Highfrequency radio interception

31. High frequency radio signals are relativelyeasy to intercept, requiring only a suitable area of land in, ideally,a "quiet" radio environment. From 1945 until the early 1980s, both NSAand GCHQ operated HF radio interception systems tasked to collect EuropeanILC communications in Scotland.(16)

32. The most advanced type of HF monitoringsystem deployed during this period for Comint purposes was a large circularantenna array known as AN/FLR-9. AN/FLR-9 antennae are more than 400 metresin diameter. They can simultaneously intercept and determine the bearingof signals from as many directions and on as many frequencies as may bedesired. In 1964, AN/FLR-9 receiving systems were installed at San Vitodei Normanni, Italy; Chicksands, England, and Karamursel, Turkey.

33. In August 1966, NSA transferredILC collection activities from its Scottish site at Kirknewton, to MenwithHill in England. Ten years later, this activity was again transferred,to Chicksands. Although the primary function of the Chicksands site wasto intercept Soviet and Warsaw Pact air force communications, it was alsotasked to collect ILC and "NDC" (Non-US Diplomatic Communications). Prominentamong such tasks was the collection of FRD traffic (i.e., French diplomaticcommunications). Although most personnel at Chicksands were members ofthe US Air Force, diplomatic and ILC interception was handled by civilianNSA employees in a unit called DODJOCC.(17)

34. During the 1970s, BritishComint units on Cyprus were tasked to collect HF communications of alliedNATO nations, including Greece and Turkey. The interception took placeat a British army unit at Ayios Nikolaos, eastern Cyprus.(18)In the United States in 1975, investigations by a US CongressionalCommittee revealed that NSA was collecting diplomatic messages sent toand from Washington from an army Comint site at Vint Hill Farms, Virginia.The targets of this station included the United Kingdom.(19)

Spaceinterception of inter-city networks

35. Long distance microwaveradio relay links may require dozens of intermediate stations to receiveand re-transmit communications. Each subsequent receiving station picksup only a tiny fraction of the original transmitted signal; the remainderpasses over the horizon and on into space, where satellites can collectit. These principles were exploited during the 1960s to provide Comintcollection from space. The nature of microwave "spillage" means that thebest position for such satellites is not above the chosen target, but upto 80 degrees of longitude away.

36. The first US Comint satellite,CANYON, was launched In August 1968, followed soon by a second. The satelliteswere controlled from a ground station at Bad Aibling, Germany. In orderto provide permanent coverage of selected targets, CANYON satellites wereplaced close to geostationary orbits. However, the orbits were not exact,causing the satellites to change position and obtain more data on groundtargets.(20)Seven CANYON satellites were launched between 1968 and 1977.

37. CANYON's target was the SovietUnion. Major Soviet communications links extended for thousands of miles,much of it over Siberia, where permafrost restricted the reliable use ofunderground cables. Geographical circumstances thus favoured NSA by makingSoviet internal communications links highly accessible. The satellitesperformed better than expected, so the project was extended.

38. The success of CANYON led to thedesign and deployment of a new class of Comint satellites, CHALET. Theground station chosen for the CHALET series was Menwith Hill, England.Under NSA project P-285, US companies were contracted to install and assistin operating the satellite control system and downlinks (RUNWAY) and groundprocessing system (SILKWORTH). The first two CHALET satellites were launchedin June 1978 and October 1979. After the name of the first satellite appearedin the US press, they were renamed VORTEX. In 1982, NSA obtained approvalfor expanded "new mission requirements" and were given funds and facilitiesto operate four VORTEX satellites simultaneously. A new 5,000m^{2}operations centre (STEEPLEBUSH) was constructed to house processing equipment.When the name VORTEX was published in 1987, the satellites were renamedMERCURY.(21)

39. The expanded mission given to MenwithHill after 1985 included MERCURY collection from the Middle East. The stationreceived an award for support to US naval operations in the Persian Gulffrom 1987 to 1988. In 1991, a further award was given for support of theIraqi war operations, Desert Storm and Desert Shield.(22)Menwith Hill is now the major US site for Comint collection against itsmajor ally, Israel. Its staff includes linguists trained in Hebrew, Arabicand Farsi as well as European languages. Menwith Hill has recently beenexpanded to include ground links for a new network of Sigint satelliteslaunched in 1994 and 1995 (RUTLEY). The name of the new class of satellitesremains unknown.

Sigintsatellites

40. The CIA developed a secondclass of Sigint satellite with complementary capabilities over the periodfrom 1967 to 1985. Initially known as RHYOLITE and later AQUACADE, thesesatellites were operated from a remote ground station in central Australia,Pine Gap. Using a large parabolic antenna which unfolded in space, RHYOLITEintercepted lower frequency signals in the VHF and UHF bands. Larger, mostrecent satellites of this type have been named MAGNUM and then ORION. Theirtargets include telemetry, VHF radio, cellular mobile phones, paging signals,and mobile data links.

41. A third class of satellite, knownfirst as JUMPSEAT and latterly as TRUMPET, operates in highly ellipticalnear-polar orbits enabling them to "hover" for long period over high northernlatitudes. They enable the United States to collect signals from transmittersin high northern latitudes poorly covered by MERCURY or ORION, and alsoto intercept signals sent to Russian communications satellites in the sameorbits.
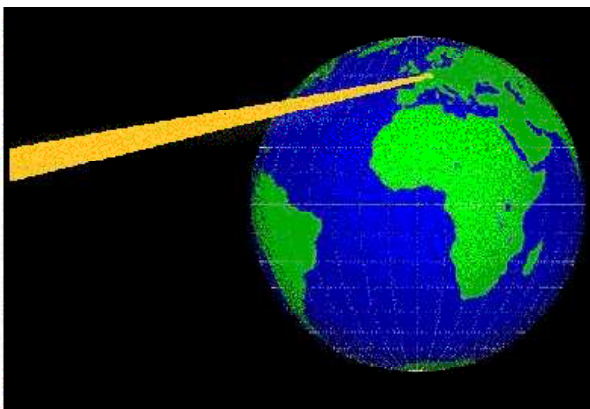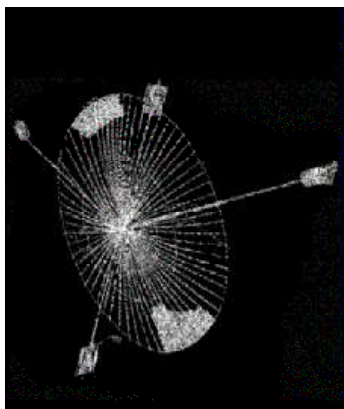
| Comint satellites in geostationaryorbits, such as VORTEX, intercept terrestial microwave spillage | Inter-city microwave radiorelay tower pills" signals into space |

42. Although precise details of US space-basedSigint satellites launched after 1990 remain obscure, it is apparent fromobservation of the relevant ground centres that collection systems haveexpanded rather than contracted. The main stations are at Buckley Field,Denver, Colorado; Pine Gap, Australia; Menwith Hill, England; and Bad Aibling,Germany. The satellites and their processing facilities are exceptionallycostly (of the order of $1 billion US each). In 1998, the US National ReconnaissanceOffice (NRO) announced plans to combine the three separate classes of Sigintsatellites into an Integrated Overhead Sigint Architecture (IOSA) in orderto " improve Sigint performance and avoid costs by consolidating systems,utilising ... new satellite and data processing technologies".(23)

43. It follows that, within constraintsimposed by budgetary limitation and tasking priorities, the United Statescan if it chooses direct space collection systems to intercept mobile communicationssignals and microwave city-to-city traffic anywhere on the planet. Thegeographical and processing difficulties of collecting messages simultaneouslyfrom all parts of the globe suggest strongly that the tasking of thesesatellites will be directed towards the highest priority national and militarytargets. Thus, although European communications passing on inter-city microwaveroutes can be collected, it is likely that they are normally ignored. Butit is very highly probable that communications to or from Europe and whichpass through the microwave communications networks of Middle Eastern statesare collected and processed.

44. No other nation (including the former Soviet Union) has deployed satellites comparable to CANYON, RHYOLITE, or their successors. Both Britain (project ZIRCON) and France (project ZENON) have attempted to do so, but neither persevered. After 1988 the British government purchased capacity on the US VORTEX (now MERCURY) constellation to use for unilateral national purposes. (24) A senior UK Liaison Officer and staff from GCHQ work at Menwith Hill NSA station and assist in tasking and operating the satellites.

COMSAT ILC collection

45. Systematic collection of COMSAT ILC communications began in 1971. Two ground stations were built for this purpose. The first at Morwenstow, Cornwall, England had two 30-metre antennae. One intercepted communications from the Atlantic Ocean Intelsat; the other the Indian Ocean Intelsat. The second Intelsat interception site was at Yakima, Washington in the northwestern United States. NSA's "Yakima Research Station" intercepted communications passing through the Pacific Ocean Intelsat satellite.

46. ILC interception capability against western-run communications satellites remained at this level until the late 1970s, when a second US site at Sugar Grove, West Virginia was added to the network. By 1980, its three satellite antenna had been reassigned to the US Naval Security Group and were used for COMSAT interception. Large-scale expansion of the ILC satellite interception system took place between 1985 and 1995, in conjunction with the enlargement of the ECHELON processing system (section 3). New stations were constructed in the United States (Sabana Seca, Puerto Rico), Canada (Leitrim, Ontario), Australia (Kojarena, Western Australia) and New Zealand (Waihopai, South Island). Capacity at Yakima, Morwenstow and Sugar Grove was expanded, and continues to expand.

Based on a simple count of the number of antennae currently installed at each COMSAT interception or satellite SIGINT station, **it appears that the UKUSA nations are between them currently operating at least 120 satellite based collection systems. The approximate number of antennae in each category are:**

- Tasked on western commercial communications satellites (ILC)	**40**
- Controlling space based signals intelligence satellites	**30**
- Currently or formerly tasked on Soviet communications satellites	**50**

Systems in the third category may have been reallocated to ILC tasks since the end of the cold war.(25)

47. Other nations increasingly collect Comint from satellites. Russia's FAPSI operates large ground collection sites at Lourdes, Cuba and at Cam Ranh Bay, Vietnam.(26) Germany's BND and France's DGSE are alleged to collaborate in the operation of a COMSAT collection site at Kourou, Guyana, targeted on "American and South American satellite communications". DGSE is also said to have COMSAT collection sites at Domme (Dordogne, France), in New Caledonia, and in the United Arab Emirates.(27) The Swiss intelligence service has recently announced a plan for two COMSAT interception stations.(28)

Satellite ground terminal at Etam, West Virginia connecting Europe and the US via Intelsat IV

GCHQ constructed an identical "shadow" station in 1972 to intercept Intelsat messages for UKUSA
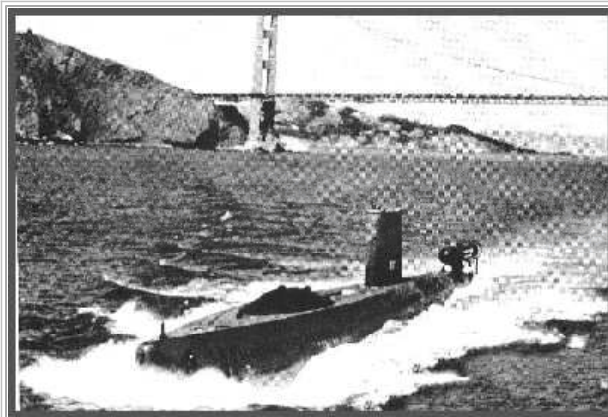
Submarine cable interception

48. Submarine cables now play a dominant role in international telecommunications, since - in contrast to the limited bandwidth available for space systems - optical media offer seemingly unlimited capacity. Save where cables terminate in countries where telecommunications operators provide Comint access (such as the UK and the US), submarine cables appear intrinsically secure because of the nature of the ocean environment.

49. In October 1971, this security was shown not to exist. A US submarine, Halibut, visited the Sea of Okhotsk off the eastern USSR and recorded communications passing on a military cable to the Khamchatka Peninsula. Halibut was equipped with a deep diving chamber, fully in view on the submarine's stern. The chamber was described by the US Navy as a "deep submergence rescue vehicle". The truth was that the "rescue vehicle" was welded immovably to the submarine. Once submerged, deep-sea divers exited the submarine and wrapped tapping coils around the cable. Having proven the principle, USS Halibut returned in 1972 and laid a high capacity recording pod next to the cable. The technique involved no physical damage and was unlikely to have been readily detectable.(29)
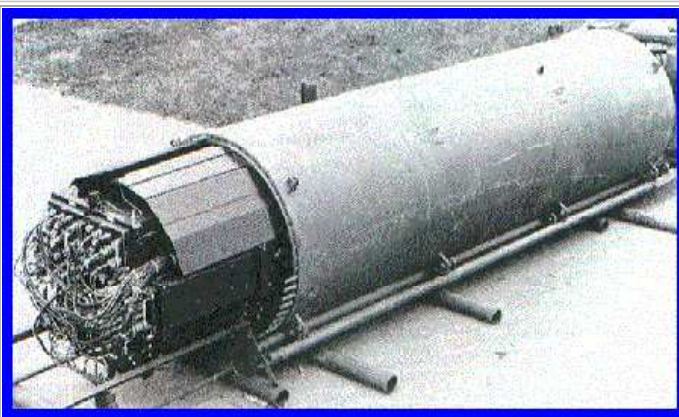
50. The Okhotsk cable tapping operation continued for ten years, involving routine trips by three different specially equipped submarines to collect old pods and lay new ones; sometimes, more than one pod at a time. New targets were added in 1979. That summer, a newly converted submarine called USS Parche travelled from San Francisco under the North Pole to the Barents Sea, and laid a new cable tap near Murmansk. Its crew received a presidential citation for their achievement. The Okhotsk cable tap ended in 1982, after its location was compromised by a former NSA employee who sold information about the tap, codenamed IVY BELLS, to the Soviet Union. One of the IVY BELLS pods is now on display in the Moscow museum of the former KGB. The cable tap in the Barents Sea continued in operation, undetected, until tapping stopped in 1992.

51. During 1985, cable-tapping operations were extended into the Mediterranean, to intercept cables linking Europe to West Africa. (30)After the cold war ended, the USS Parche was refitted with an extended section to accommodate larger cable tapping equipment and pods. Cable taps could be laid by remote control, using drones. USS Parche continues in operation to the present day, but the precise targets of its missions remain unknown. The Clinton administration evidently places high value on its achievements, Every year from 1994 to 1997, the submarine crew has been highly commended.(31)Likely targets may include the Middle East, Mediterranean, eastern Asia, and South America. The United States is the only naval power known to have deployed deep-sea technology for this purpose.

52. Miniaturised inductive taps recorders have also been used to intercept underground cables.(32)Optical fibre cables, however, do not leak radio frequency signals and cannot be tapped using inductive loops. NSA and other Comint agencies have spent a great deal of money on research into tapping optical fibres, reportedly with little success. But long distance optical fibre cables are not invulnerable. The key means of access is by tampering with optoelectronic "repeaters" which boost signal levels over long distances. It follows that any submarine cable system using submerged optoelectronic repeaters cannot be considered secure from interception and communications intelligence activity.

USS halibut with disguised chamber for diving	*Cable tapping pod laid by US submarine off Khamchatka*

Intercepting the Internet

53. The dramatic growth in the size and significance of the Internet and of related forms of digital communications has been argued by some to pose a challenge for Comint agencies. This does not appear correct. During the 1980s, NSA and its UKUSA partners operated a larger international communications network than the then Internet but based on the same technology.(33)According to its British partner "all GCHQ systems are linked together on the largest LAN [Local Area Network] in Europe, which is connected to other sites around the world via one of the largest WANs [Wide Area Networks] in the world ... its main networking protocol is Internet Protocol (IP).(34)This global network, developed as project EMBROIDERY, includes PATHWAY, the NSA's main computer communications network. It provides fast, secure global communications for ECHELON and other systems.

54. Since the early 1990s, fast and sophisticated Comint systems have been developed to collect, filter and analyse the forms of fast digital communications used by the Internet. Because most of the world's Internet capacity lies within the United States or connects to the United States, many communications in "cyberspace" will pass through intermediate sites within the United States. Communications from Europe to and from Asia, Oceania, Africa or South America normally travel via the United States.

55. Routes taken by Internet "packets" depend on the origin and destination of the data, the systems

55. Routes taken by Internet "packets"depend on the origin and destination of the data, the systems through whichthey enter and leaves the Internet, and a myriad of other factors includingtime of day. Thus, routers within the western United States are at theirmost idle at the time when central European traffic is reaching peak usage.It is thus possible (and reasonable) for messages travelling a short distancein a busy European network to travel instead, for example, via Internetexchanges in California. It follows that a large proportion of internationalcommunications on the Internet will by the nature of the system pass throughthe United States and thus be readily accessible to NSA.

56.Standard Internet messages are composedof packets called "datagrams" . Datagrams include numbers representingboth their origin and their destination, called "IP addresses". The addressesare unique to each computer connected to the Internet. They are inherentlyeasy to identify as to country and site of origin and destination. Handling,sorting and routing millions of such packets each second is fundamentalto the operation of major Internet centres. The same process facilitatesextraction of traffic for Comint purposes.

57. Internet traffic can be accessedeither from international communications links entering the United States,or when it reaches major Internet exchanges. Both methods have advantages.Access to communications systems is likely to be remain clandestine - whereasaccess to Internet exchanges might be more detectable but provides easieraccess to more data and simpler sorting methods. Although the quantitiesof data involved are immense, NSA is normally legally restricted to lookingonly at communications that start or finish in a foreign country. Unlessspecial warrants are issued, all other data should normally be thrown awayby machine before it can be examined or recorded.

58. Much other Internet traffic (whetherforeign to the US or not) is of trivial intelligence interest or can behandled in other ways. For example, messages sent to "Usenet" discussiongroups amounts to about 15 Gigabytes (GB) of data per day; the rough equivalentof 10,000 books. All this data is broadcast to anyone wanting (or willing)to have it. Like other Internet users, intelligence agencies have opensource access to this data and store and analyse it. In the UK, the DefenceEvaluation and Research Agency maintains a 1 Terabyte database containingthe previous 90 days of Usenet messages.(35)A similar service, called "Deja News", is available to users of the WorldWide Web (WWW). Messages for Usenet are readily distinguishable. It ispointless to collect them clandestinely.

59. Similar considerations affect theWorld Wide Web, most of which is openly accessible. Web sites are examinedcontinuously by "search engines" which generate catalogues of their contents."Alta Vista" and "Hotbot" are prominent public sites of this kind. NSAsimilarly employs computer "bots" (robots) to collect data of interest.For example, a New York web site known as JYA.COM (http://www.jya.com/crypto.htm)offers extensive public information on Sigint, Comint and cryptography.The site is frequently updated. Records of access to the site show thatevery morning it is visited by a "bot" from NSA's National Computer SecurityCentre, which looks for new files and makes copies of any that it finds.(36)

60. It follows that foreign Internettraffic of communications intelligence interest - consisting of e-mail,file transfers, "virtual private networks" operated over the internet,and some other messages - will form at best a few per cent of the trafficon most US Internet exchanges or backbone links. According to a formeremployee, NSA had by 1995 installed "sniffer" software to collect suchtraffic at nine major Internet exchange points (IXPs).(37)The first two such sites identified, FIX East and FIX West, are operatedby US government agencies. They are closely linked to nearby commerciallocations, MAE East and MAE West (see table). Three other sites listedwere Network Access Points originally developed by the US National ScienceFoundation to provide the US Internet with its initial "backbone".

Internetsite	Location	Operator	Designation
FIX East	CollegePark, Maryland	US government	FederalInformation Exchange
FIX West	MountainView, California	US government	FederalInformation Exchange
MAE East	Washington,DC	MCI	MetropolitanArea Ethernet
New YorkNAP	Pennsauken,New Jersey	Sprintlink	NetworkAccess Point
SWAB	Washington,DC	PSInet /Bell Atlantic	SMDS WashingtonArea Bypass
ChicagoNAP	Chicago,Illinois	Ameritech/ Bellcorp	NetworkAccess Point
San FranciscoNAP	San Francisco,California	PacificBell	NetworkAccess Point
MAE West	San Jose,California	MCI	MetropolitanArea Ethernet
CIX	Santa ClaraCalifornia	CIX	CommercialInternet Exchange

Table 1 NSA Internet Comint accessat IXP sites (1995) (38)

61. The same article alleged that a leadingUS Internet and telecommunications company had contracted with NSA to developsoftware to capture Internet data of interest, and that deals had beenstruck with the leading manufacturers Microsoft, Lotus, and Netscape toalter their products for foreign use. The latter allegation has provencorrect (see technical annexe). Providing such features would make littlesense unless NSA had also arranged general access to Internet traffic.Although NSA will not confirm or deny such allegations, a 1997 court casein Britain involving alleged "computer hacking" produced evidence of NSAsurveillance of the Internet. Witnesses from the US Air Force componentof NSA acknowledged using packet sniffers and specialised programmes totrack attempts to enter US military computers. The case collapsed afterthe witnesses refused to provide evidence about the systems they had used.(39)

Covertcollection of high capacity signals

62. Where access to signals of interestis not possible by other means, Comint agencies have constructed specialpurpose interception equipment to install in embassies or other diplomaticpremises, or even to carry by hand to locations of special interest. Extensivedescriptions of operations of this kind have been published by Mike Frost,a former official of CSE, the Canadian Sigint agency.(40)Although city centre embassy premises are often ideally situated to intercepta wide range

of communications, ranging from official carphone servicesto high capacity microwave links,

of communications, ranging from official carphone servicesto high capacity microwave links, processing and passing on such informationmay be difficult. Such collection operations are also highly sensitivefor diplomatic reasons. Equipment for covert collection is therefore specialised,selective and miniaturised.

63. A joint NSA/CIA "Special CollectionService" manufactures equipment and trains personnel for covert collectionactivities One major device is a suitcase-sized computer processing system.ORATORY. ORATORY is in effect a miniaturised version of the Dictionarycomputers described in the next section, capable of selecting non-verbalcommunications of interest from a wide range of inputs, according to pre-programmedselection criteria. One major NSA supplier ("The IDEAS Operation") nowoffers micro-miniature digital receivers which can simultaneously processSigint data from 8 independent channels. This radio receiver is the sizeof a credit card. It fits in a standard laptop computer. IDEAS claim, reasonably,that their tiny card "performs functions that would have taken a rack fullof equipment not long ago".

Newsatellite networks

64. New network operators have constructedmobile phone systems providing unbroken global coverage using satellitesin low or medium level earth orbits. These systems are sometimes calledsatellite personal communications systems (SPCS). Because each satellitecovers only a small area and moves fast, large numbers of satellites areneeded to provide continuous global coverage. The satellites can relaysignals directly between themselves or to ground stations. The first suchsystem to be completed, Iridium, uses 66 satellites and started operationsin 1998. Iridium appears to have created particular difficulties for communicationsintelligence agencies, since the signals down from the Iridium and similarnetworks can only be received in a small area, which may be anywhere onthe earth's surface.

3. ECHELON and Comintproduction

65. The ECHELON system became well knownfollowing publication of the previous STOA report. Since then, new evidenceshows that ECHELON has existed since the 1970s, and was greatly enlargedbetween 1975 and 1995. Like ILC interception, ECHELON has developed fromearlier methods. This section includes new information and documentaryevidence about ECHELON and satellite interception.

The"Watch List"

66. After the public revelation ofthe SHAMROCK interception programme, NSA Director Lt General Lew Allendescribed how NSA used "'watch lists" as an aid to watch for foreign activityof reportable intelligence interest".(41)"We have been providing details ... of any messages contained in the foreigncommunications we intercept that bear on named individuals or organisations.These compilations of names are commonly referred to as 'Watch Lists'",he said.(42)Until the 1970s, Watch List processing was manual. Analysts examined interceptedILC communications, reporting, "gisting" or analysing those which appearedto cover names or topics on the Watch List.

Newinformation about ECHELON sites and systems

67. It now appears that the systemidentified as ECHELON has been in existence for more than 20 years. Theneed for such a system was foreseen in the late 1960s, when NSA and GCHQplanned ILC satellite interception stations at Mowenstow and Yakima. Itwas expected that the quantity of messages intercepted from the new satelliteswould be too great for individual examination. According to former NSAstaff, the first ECHELON computers automated Comint processing at thesesites.(43)

68. NSA and CIA then discovered thatSigint collection from space was more effective than had been anticipated,resulting in accumulations of recordings that outstripped the availablesupply of linguists and analysts. Documents show that when the SILKWORTHprocessing systems was installed at Menwith Hill for the new satellites,it was supported by ECHELON 2 and other databanks (see illustration).

69. By the mid 1980s, communicationsintercepted at these major stations were heavily sifted, with a wide varietyof specifications available for non-verbal traffic. Extensive further automationwas planned in the mid 1980s as NSA Project P-415. Implementation of thisproject completed the automation of the previous Watch List activity. From1987 onwards, staff from international Comint agencies travelled to theUS to attended training courses for the new computer systems.

70. Project P-415/ECHELON made heavyuse of NSA and GCHQ's global Internet-like communication network to enableremote intelligence customers to task computers at each collection site,and receive the results automatically. The key component of the systemare local "Dictionary" computers, which store an extensive database onspecified targets, including names, topics of interest, addresses, telephonenumbers and other selection criteria. Incoming messages are compared tothese criteria; if a match is found, the raw intelligence is forwardedautomatically. Dictionary computers are tasked with many thousands of differentcollection requirements, described as "numbers" (four digit codes).

71. Tasking and receiving intelligencefrom the Dictionaries involves processes familiar to anyone who has usedthe Internet. Dictionary sorting and selection can be compared to usingsearch engines, which select web pages containing key words or terms andspecifying relationships. The forwarding function of the Dictionary computersmay be compared to e-mail. When requested, the system will provide listsof communications matching each criterion for review, analysis, "gisting"or forwarding. An important point about the new system is that before ECHELON,different countries and different stations knew what was being interceptedand to whom it was sent. Now, all but a fraction of the messages selectedby Dictionary computers at remote sites are forwarded to NSA or other customerswithout being read locally.
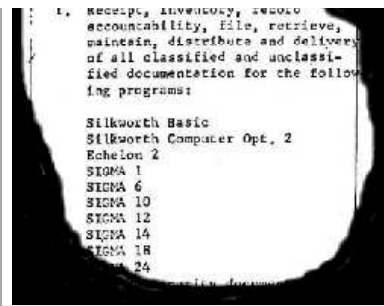
List of intelligencedatabanks operating at ECHELON Menwith Hill in 1979 included the secondgeneration of ECHELON	*Satellite interceptionsite at Sugar Grove, West Virginia, showing six antennae targeted on Europeanand Atlantic Ocean regional communicationssatellites*

Westminster,London - Dictionary computer

72. In 1991, a British television programmereported on the operations of the Dictionary computer at GCHQ's Westminster,London office. The system "secretly intercepts every single telex whichpasses into, out of or through London; thousands of diplomatic, businessand personal messages every day. These are fed into a programme known as`Dictionary'. It picks out keywords from the mass of Sigint, and huntsout hundreds of individuals and corporations".(44)The programme pointed out that the Dictionary computers, although controlledand tasked by GCHQ, were operated by security vetted staff employed byBritish Telecom (BT), Britain's dominant telecommunications operator.(45)The presence of Dictionary computers has also been confirmed at Kojarena,Australia; and at GCHQ Cheltenham, England.(46)

SugarGrove, Virginia - COMSAT interception at ECHELON site

73. US government documents confirm thatthe satellite receiving station at Sugar Grove, West Virginia is an ECHELONsite, and that collects intelligence from COMSATs. The station is about250 miles south-west of Washington, in a remote area of the ShenandoahMountains. It is operated by the US Naval Security Group and the US AirForce Intelligence Agency.

74. An upgraded system called TIMBERLINEII, was installed at Sugar Grove in the summer of 1990. At the same time,according to official US documents, an "ECHELON training department" wasestablished.(47)With training complete, the task of the station in 1991 became "to maintainand operate an ECHELON site".(48)

75. The US Air Force has publicly identifiedthe intelligence activity at Sugar Grove: its "mission is to direct satellitecommunications equipment [in support of] consumers of COMSAT information...This is achieved by providing a trained cadre of collection systemoperators, analysts and managers".(49)In 1990, satellite photographs showed that there were 4 satellite antennaeat Sugar Grove. By November 1998, ground inspection revealed that thishad expanded to a group of 9.

SabanaSeca, Puerto Rico and Leitrim, Canada - COMSAT interception sites

76. Further information published by theUS Air Force identifies the US Naval Security Group Station at Sabana Seca,Puerto Rico as a COMSAT interception site. Its mission is "to become thepremier satellite communications processing and analysis field station".(50)

77. Canadian Defence Forces have publisheddetails about staff functions at the Leitrim field station of the CanadianSigint agency CSE. The station, near Ottawa, Ontario has four satelliteterminals, erected since 1984. The staff roster includes seven CommunicationsSatellite Analysts, Supervisors and Instructors.(51)

78. In a publicly available resume,a former Communication Satellite Analyst employed at Leitrim describeshis job as having required expertise in the "operation and analysis ofnumerous Comsat computer systems and associated subsystems ... [utilising]computer assisted analysis systems ... [and] a broad range of sophisticatedelectronic equipment to intercept and study foreign communications andelectronic transmissions.(52)Financial reports from CSE also indicate that in 1995/96, the agency plannedpayments of $7 million to ECHELON and $6 million to Cray (computers). Therewere no further details about ECHELON.(53)

Waihopai,New Zealand - Intelsat interception at ECHELON site

79. New Zealand's Sigint agency GCSB operatestwo satellite interception terminals at Waihopai, tasked on Intelsat satellitescovering the Pacific Ocean. Extensive details have already been publishedabout the station's Dictionary computers and its role in the ECHELON network.(54)After the book was published, a New Zealand TV station obtained imagesof the inside of the station operations centre. The pictures were obtainedclandestinely by filming through partially curtained windows at night.The TV reporter was able to film close-ups of technical manuals held inthe control centre. These were Intelsat technical manuals, providing confirmationthat the station targeted these satellites Strikingly, the station wasseen to be virtually empty, operating fully automatically. One guard wasinside, but was unaware he was being filmed.(55)

ILC processing techniques

80. The technical annexe describes themain systems used to extract and process communications intelligence. Thedetailed explanations given about processing methods are not essentialto understanding the core of this report, but are provided so that readersknowledgeable about telecommunications may fully evaluate the state ofthe art.

81. Fax messages and computer data(from modems) are given priority in processing because of the

81. Fax messages and computer data(from modems) are given priority in processing because of the ease withwhich they are understood and analysed. The main method of filtering andanalysing non-verbal traffic, the Dictionary computers, utilise traditionalinformation retrieval techniques, including keywords. Fast special purposechips enable vast quantities of data to be processed in this way. The newesttechnique is "topic spotting". The processing of telephone calls is mainlylimited to identifying call-related information, and traffic analysis.Effective voice "wordspotting" systems do not exist are not in use, despitereports to the contrary. But "voiceprint" type speaker identification systemshave been in use since at least 1995. The use of strong cryptography isslowly impinging on Comint agencies' capabilities. This difficulty forComint agencies has been offset by covert and overt activities which havesubverted the effectiveness of cryptographic systems supplied from and/orused in Europe.

82. The conclusions drawn in the annexeare that Comint equipment currently available has the capability, as tasked,to intercept, process and analyse every modern type of high capacity communicationssystem to which access is obtained, including the highest levels of theInternet. There are few gaps in coverage. The scale, capacity and speedof some systems is difficult fully to comprehend. Special purpose systemshave been built to process pager messages, cellular mobile radio and newsatellites.

4. Comint and Law Enforcement

83. In 1990 and 1991, the US governmentbecame concerned that the marketing of a secure telephone system by AT&Tcould curtail Comint activity. AT&T was persuaded to withdraw its product.In its place the US government offered NSA "Clipper" chips for incorporationin secure phones. The chips would be manufactured by NSA, which would alsorecord built-in keys and pass this information to other government agenciesfor storage and, if required, retrieval. This proposal proved extremelyunpopular, and was abandoned. In its place, the US government proposedthat non government agencies should be required to keep copies of everyuser's keys, a system called "key escrow" and, later, "key recovery". Viewedin retrospect, the actual purpose of these proposals was to provide NSAwith a single (or very few) point(s) of access to keys, enabling them tocontinue to access private and commercial communications.

Misrepresentation of law enforcementinterception requirements

84. Between 1993 to 1998, the United Statesconducted sustained diplomatic activity seeking to persuade EU nationsand the OECD to adopt their "key recovery" system. Throughout this period,the US government insisted that the purpose of the initiative was to assistlaw enforcement agencies. Documents obtained for this study suggest thatthese claims wilfully misrepresented the true intention of US policy. Documentsobtained under the US Freedom of Information Act indicate that policymakingwas led exclusively by NSA officials, sometimes to the complete exclusionof police or judicial officials. For example, when the specially appointedUS "Ambassador for Cryptography", David Aaron, visited Britain on 25 November1996, he was accompanied and briefed by NSA's most senior representativein Britain, Dr James J Hearn, formerly Deputy Director of NSA. Mr Aaronhad did not meet or consult FBI officials attached to his Embassy. Hismeeting with British Cabinet officials included NSA's representative andstaff from Britain's GCHQ, but police officers or justice officials fromboth nations were excluded.

85. Since 1993, unknown to Europeanparliamentary bodies and their electors, law enforcement officials frommany EU countries and most of the UKUSA nations have been meeting annuallyin a separate forum to discuss their requirements for intercepting communications.These officials met under the auspices of a hitherto unknown organisation,ILETS (International Law Enforcement Telecommunications Seminar). ILETSwas initiated and founded by the FBI. Table 2 lists ILETS meetings heldbetween 1993 and 1997.

86. At their 1993 and 1994 meetings,ILETS participants specified law enforcement user requirements for communicationsinterception. These appear in a 1974 ILETS document called "IUR 1.0". Thisdocument was based on an earlier FBI report on "Law Enforcement Requirementsfor the Surveillance of Electronic Communications", first issued in July1992 and revised in June 1994. The IUR requirement differed little in substancefrom the FBI's requirements but was enlarged, containing ten requirementsrather than nine. IUR did not specify any law enforcement need for "keyescrow" or "key recovery". Cryptography was mentioned solely in the contextof network security arrangements.

87. Between 1993 and 1997 police representativesfrom ILETS were not involved in the NSA-led policy making process for "keyrecovery", nor did ILETS advance any such proposal, even as late as 1997.Despite this, during the same period the US government repeatedly presentedits policy as being motivated by the stated needs of law enforcement agencies.At their 1997 meeting in Dublin, ILETS did not alter the IUR. It was notuntil 1998 that a revised IUR was prepared containing requirements in respectof cryptography. It follows from this that the US government misled EUand OECD states about the true intention of its policy.

88. This US deception was, however,clear to the senior Commission official responsible for information security.In September 1996, David Herson, head of the EU Senior Officers' Groupon Information Security, stated his assessment of the US "key recovery"project :

> "'*Law Enforcement*' *is a protectiveshield for all the other governmental activities ... We're talking aboutforeign intelligence, that's what all this is about. There is no question[that]* '*law enforcement*' *is a smoke screen*".(56)

89. It should be noted that technically,legally and organisationally, law enforcement requirements for communicationsinterception differ fundamentally from communications intelligence. Lawenforcement agencies (LEAs) will normally wish to intercept a specificline or group of lines, and must normally justify their requests to a judicialor administrative authority before proceeding. In contract, Comint agenciesconduct broad international communications "trawling" activities, and operateunder general warrants. Such operations do not require or even supposethat the parties they intercept are criminals.

Such distinctions are vitalto civil liberty, but risk being eroded it the boundaries between law

Such distinctions are vitalto civil liberty, but risk being eroded it the boundaries between law enforcementand communications intelligence interception becomes blurred in future.

Year	Venue	Non-EUparticipants	EU participants
1993	Quantico,Virginia, USA	Australia,Canada, Hong Kong, Norway United States	Denmark,France, Germany, Netherlands, Spain, Sweden, United Kingdom
1994	Bonn, Germany	Australia,Canada, Hong Kong, Norway, United States	Austria,Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Luxembourg,Netherlands, Portugal, Spain, Sweden, United Kingdom
1995	Canberra,Australia	Australia,Canada, Hong Kong, New Zealand, Norway, United States	Belgium,France, Germany, Greece, Ireland, Italy, Netherlands, Spain, Sweden, UnitedKingdom
1997	Dublin,Ireland	Australia,Canada, Hong Kong, New Zealand, Norway, United States	Austria,Belgium, Denmark, Finland, France, Germany, Ireland, Italy, Luxembourg,Netherlands, Portugal, Spain, Sweden, United Kingdom

Table 2 ILETS meetings, 1993-1997

Law enforcement communications interception- policy development in Europe

90. Following the second ILETS meetingin Bonn in 1994, IUR 1.0 was presented to the Council of Ministers andwas passed without a single word being altered on 17January 1995.(57)During 1995, several non EU members of the ILETS group wrote to the Councilto endorse the (unpublished) Council resolution. The resolution was notpublished in the Official Journal for nearly two years, on 4 November 1996.

91. Following the third ILETS meetingin Canberra in 1995, the Australian government was asked to present theIUR to International Telecommunications Union (ITU). Noting that "law enforcementand national security agencies of a significant number of ITU member stateshave agreed on a generic set of requirements for legal interception", theAustralian government asked the ITU to advise its standards bodies to incorporatethe IUR requirements into future telecommunications systems on the basisthat the "costs of [providing] legal interception capability and associateddisruptions can be lessened by providing for that capability at the designstage".(58)

92. It appears that ILETS met againin 1998 and revised and extended its terms to cover the Internet and SatellitePersonal Communications Systems such as Iridium. The new IUR also specified"additional security requirements for network operators and service providers",extensive new requirements for personal information about subscribers,and provisions to deal with cryptography.

93. On 3 September 1998, the revisedIUR was presented to the Police Co-operation Working Group as ENFOPOL 98.The Austrian Presidency proposed that, as in 1994, the new IUR be adoptedverbatim as a Council Resolution on interception "in respect of new technology".(59)The group did not agree. After repeated redrafting, a fresh paper has beenprepared by the German Presidency, for the eventual consideration of CouncilHome and Justice ministers.(60)

5. Comint and economicintelligence

94. During the 1998 EP debate on "Transatlanticrelations/ECHELON system" Commissioner Bangeman observed on behalf of theCommission that "If this system were to exist, it would be an intolerableattack against individual liberties, competition and the security of thestates".(61)The existence of ECHELON was described in section 3, above. This sectiondescribes the organisational and reporting frameworks within which economicallysensitive information collected by ECHELON and related systems is disseminated,summarising examples where European organisations have been the subjectof surveillance.

Tasking economic intelligence

95. US officials acknowledge that NSAcollects economic information, whether intentionally or otherwise. Formermilitary intelligence attaché Colonel Dan Smith worked at the USEmbassy, London until 1993. He regularly received Comint product from MenwithHill. In 1998, he told the BBC that at Menwith Hill:

> *"In terms of scooping up communications,inevitably since their take is broadband, there will be conversations orcommunications which are intercepted which have nothing to do with themilitary, and probably within those there will be some information aboutcommercial dealings"*

"Anything would be possible technically.Technically they can scoop all this information up, sort through it andfind out what it is that might be asked for . . . But there is not policyto do this specifically in response to a particular company's interest(62)

96. In general, this statement is notincorrect. But it overlooks fundamental distinctions between tasking anddissemination, and between commercial and economic intelligence. Thereis no evidence that companies in any of the UKUSA countries are able totask Comint collection to suit their private purposes. They do not haveto. Each UKUSA country authorises national level intelligence assessmentorganisations and relevant individual ministries to task and receive economicintelligence from Comint. Such information may be collected for myriadpurposes, such as: estimation of future essential commodity prices; determiningother nation's private positions in trade negotiations; monitoring internationaltrading in arms; tracking sensitive technology; or evaluating the politicalstability and/or economic strength of a target country. Any of these targetsand many others may produce intelligence of direct commercial relevance.The decision as to whether it should be disseminated or exploited is takennot by Comint agencies but by national government organisation(s).

Disseminatingeconomic intelligence

97. In 1970, according to its former ExecutiveDirector, the US Foreign Intelligence Advisory Board

97. In 1970, according to its former ExecutiveDirector, the US Foreign Intelligence Advisory Board recommended that "henceforthe economic intelligence be considered a function of the national security,enjoying a priority equivalent to diplomatic, military, technological intelligence".(63)On 5 May 1977, a meeting between NSA, CIA and the Department of Commerceauthorised the creation of secret new department, the "Office of IntelligenceLiaison". Its task was to handle "foreign intelligence" of interest tothe Department of Commerce. Its standing orders show that it was authorisedto receive and handle SCI intelligence - Comint and Sigint from NSA. Thecreationof this office THUS provided a formal mechanism whereby NSA data couldbe used to support commercial and economic interests. After this systemwas highlighted in a British TV programme in 1993, its name was changedto the "Office of Executive Support".(64)Also in 1993, President Clinton extended US intelligence support to commercialorganisations by creating a new National Economic Council, parallelingthe National Security Council.

98. The nature of this intelligencesupport has been widely reported. "Former intelligence officials and otherexperts say tips based on spying ... regularly flow from the Commerce Departmentto U.S. companies to help them win contracts overseas.(65)The Office of Executive Support provides classified weekly briefings tosecurity officials. One US newspaper obtained reports from the CommerceDepartment demonstrating intelligence support to US companies:

> One such document consists ofminutes from an August 1994 Commerce Department meeting [intended] to identifymajor contracts open for bid in Indonesia in order to help U.S. companieswin the work. A CIA employee ... spoke at the meeting; five of the 16 peopleon the routine distribution list for the minutes were from the CIA.

99. In the United Kingdom, GCHQ is specificallyrequired by law (and as and when tasked by the British government) to interceptforeign communications "in the interests of the economic well-being ofthe United Kingdom ...in relation to the actions or intentions of personsoutside the British Islands". Commercial interception is tasked and analysedby GCHQ's K Division. Commercial and economic targets can be specifiedby the government's Overseas Economic Intelligence Committee, the EconomicStaff of the Joint Intelligence Committee, the Treasury, or the Bank ofEngland.(66)According to a former senior JIC official, the Comint take routinely includes"company plans, telexes, faxes, and transcribed phone calls. Many werecalls between Europe and the South[ern Hemisphere]".(67)

100. In Australia, commercially relevantComint is passed by DSD to the Office of National Assessments, who considerwhether, and if so where, to disseminate it. Staff there may pass informationto Australian companies if they believe that an overseas nation has orseeks an unfair trade advantage. Targets of such activity have includedThomson-CSF, and trade negotiations with Japanese purchasers of coal andiron ore. Similar systems operate in the other UKUSA nations, Canada andNew Zealand.

The use of Comint economicintelligence product

PanaviaEuropean Fighter Aircraft consortium and Saudi Arabia

101. In 1993, former National SecurityCouncil official Howard Teicher described in a programme about MenwithHill how the European Panavia company was specifically targeted over salesto the Middle East. "I recall that the words 'Tornado' or 'Panavia' - informationrelated to the specific aircraft - would have been priority targets thatwe would have wanted information about".(68)

ThomsonCSF and Brazil

102. In 1994, NSA intercepted phone callsbetween Thomson-CSF and Brazil concerning SIVAM, a $1.3 billion surveillancesystem for the Amazon rain forest. The company was alleged to have bribedmembers of the Brazilian government selection panel. The contract was awardedto the US Raytheon Corporation - who announced afterwards that "the Departmentof Commerce worked very hard in support of U.S. industry on this project".(69)Raytheon also provide maintenance and engineering services to NSA's ECHELONsatellite interception station at Sugar Grove.

AirbusIndustrie and Saudi Arabia

103. According to a well-informed 1995press report :"from a commercial communications satellite, NSA lifted allthe faxes and phone calls between the European consortium Airbus, the Saudinational airline and the Saudi government. The agency found that Airbusagents were offering bribes to a Saudi official. It passed the informationto U.S. officials pressing the bid of Boeing Co and McDonnell Douglas Corp.,which triumphed last year in the $6 billion competition." (70)

Internationaltrade negotiations

104. Many other accounts have been publishedby reputable journalists and some firsthand witnesses citing frequent occasionson which the US government has utlitised Comint for national commercialpurposes. These include targeting data about the emission standards ofJapanese vehicles;(71)1995 trade negotiations the import of Japanese luxury cars;(72)French participation in the GATT trade negotiations in 1993; the Asian-PacificEconomic Conference (APEC), 1997.

Targeting host nations

105. The issue of whether the United Statesutilises communications intelligence facilities such as Menwith Hilll orBad Aibling to attack host nations' communications also arises. The availableevidence suggests that such conduct may normally be avoided. Accordingto former National Security Council official Howard Teicher, the US governmentwould not direct NSA to spy on a host governments such as Britain:

> " [But] I would never say neverin this business because, at the end of the day, national interests arenational interests ... sometimes our interests diverge. So never say never- especially in this business"

.

6. Comint capabilities after2000

Developments in technology

106. Since the mid-1990s, communicationsintelligence agencies have faced substantial difficulties in maintainingglobal access to communications systems. These difficulties will increaseduring and after 2000. The major reason is the shift in telecommunicationsto high capacity optical fibre networks. Physical access to cables is requiredfor interception. Unless a fibre network lies within or passes througha collaborating state, effective interception is practical only by tamperingwith optoelectronic repeaters (when installed). This limitation is likelyto place many foreign land-based high capacity optical fibre networks beyondreach. The physical size of equipment needed to process traffic, togetherwith power, communications and recording systems, makes clandestine activityimpractical and risky.

107. Even where access is readily available(such as to COMSATs), the proliferation of new systems will limit collectionactivities, partly because budgetary constraint will restrict new deployments,and partly because some systems (for example, Iridium) cannot be accessedby presently available systems.

108. In the past 15 years the substantialtechnological lead in computers and information technology once enjoyedby Comint organisations has all but disappeared. Their principal computersystems are bought "off the shelf" and are the equal of or even inferiorto those used by first rank industrial and academic organisations. Theydiffer only in being "TEMPEST shielded", preventing them emitting radiosignals which could be used to analyse Sigint activity.

109. Communications intelligence organisationsrecognise that the long war against civil and commercial cryptography hasbeen lost. A thriving academic and industrial community is skilled in cryptographyand cryptology. The Internet and the global marketplace have created afree flow in information, systems and software. NSA has failed in its missionto perpetuate access by pretending that that "key escrow" and like systemswere intended to support law enforcement (as opposed to Comint) requirements.

110. Future trends in Comint are likelyto include limits on investment in Comint collection from space; greateruse of human agents to plant collection devices or obtain codes than inthe past; and an intensified effort to attack foreign computer systems,using the Internet and other means (in particular, to gain access to protectedfiles or communications before they are encrypted).

111. Attempts to restrict cryptographyhave nevertheless delayed the large-scale introduction of effective cryptographicsecurity systems. The reduced cost of computational power has also enabledComint agencies to deploy fast and sophisticated processing and sortingtools.

112. Recent remarks to CIA veteransby the head of staff of the US House of Representatives Permanent SelectCommittee on Intelligence, ex CIA officer John Millis illustrate how NSAviews the same issues:

> "*Signals intelligence is in acrisis. ... Over the last fifty years ... In the past, technology has beenthe friend of NSA, but in the last four or five years technology has movedfrom being the friend to being the enemy of Sigint.*

The media of telecommunicationsis no longer Sigint-friendly. It used to be. When you were doing RF signals,anybody within range of that RF signal could receive it just as clearlyas the intended recipient. We moved from that to microwaves, and peoplefigured out a great way to harness that as well. Well, we're moving tomedia that are very difficult to get to.

Encryption is here and it's goingto grow very rapidly. That is bad news for Sigint ... It is going to takea huge amount of money invested in new technologies to get access and tobe able to break out the information that we still need to get from Sigint".

Policy issues for the European Parliament

1. The 1998 Parliamentary resolutionon "Transatlantic relations/ECHELON system"(73)called for "protective measures concerning economic information and effectiveencryption". Providing such measures may be facilitated by developing anin-depth understanding of present and future Comint capabilities.

2. At the technical level, protectivemeasures may best be focused on defeating hostile Comint activity by denyingaccess or, where this is impractical or impossible, preventing processingof message content and associated traffic information by general use ofcryptography.

3. As the SOGIS group withinthe Commission has recognised,(74)the contrasting interests of states is a complex issue. Larger states havemade substantial investments in Comint capabilities. One member state isactive in the UKUSA alliance, whilst others are either "third parties"to UKUSA or have made bilateral arrangements with NSA. Some of these arrangementswere a legacy of the cold war; others are enduring. These issues createinternal and international conflicts of interest. Technical solutions arenot obvious. It should be possible to define a shared interest in implementingmeasures to defeat future external Comint activities directed against Europeanstates, their citizens and commercial activities.

4. A second area of apparentconflict concerns states' desires to provide communications interceptionfor legitimate law enforcement purposes. The technical and legal processesinvolved in providing interception for law enforcement purpose differ fundamentallyfrom those used in communications intelligence. Partly because of the lackof parliamentary and public awareness of Comint activities, this distinctionis often glossed over, particularly by states that invest heavily in Comint.Any failure to distinguish between legitimate law enforcement interceptionrequirements and interception for clandestine intelligence purposes raisesgrave issues for civil liberties. A clear boundary between law enforcementand "national security" interception activity is essential to the protectionof human rights and fundamental freedoms.

5. At the present time, Internetbrowsers and other software used in almost every personal computer in

5. At the present time, Internetbrowsers and other software used in almost every personal computer in Europeis deliberately disabled such that "secure" communications they send can,if collected, be read without difficulty by NSA. US manufacturers are compelledto make these arrangements under US export rules. A level playing fieldis important. Consideration could be given to a countermeasure whereby,if systems with disabled cryptographic systems are sold outside the UnitedStates, they should be required to conform to an "open standard" such thatthird parties and other nations may provide additional applications whichrestore the level of security to at least enjoyed by domestic US customers.

6. The work of ILETS has proceededfor 6 years without the involvement of parliaments, and in the absenceof consultation with the industrial organisations whose vital intereststheir work affects. It is regrettable that, prior to the publication ofthis report, public information has not been available in states aboutthe scope of the policy-making processes, inside and outside the EU, whichhave led to the formulation of existing and new law enforcement "user requirements".As a matter of urgency, the current policy-making process should be madeopen to public and parliamentary discussion in member states and in theEP, so that a proper balance may be struck between the security and privacyrights of citizens and commercial enterprises, the financial and technicalinterests of communications network operators and service providers, andthe need to support law enforcement activities intended to suppress seriouscrime and terrorism.

Technical annexe

Broadband (high capacity multi-channel)communications

1. From 1950 until the early 1980s, highcapacity multi-channel analogue communications systems were usually engineeredusing separate communications channels carried at different frequenciesThe combined signal, which could include 2,000 or more speech channels,was a "multiplex". The resulting "frequency division multiplex" (FDM) signalwas then carried on a much higher frequency, such as by a microwave radiosignal.

2. Digital communications have almostuniversally taken over from analogue methods. The basic system of digitalmulti-channel communications is time division multiplexing (TDM). In aTDM telephony system, the individual conversational channels are firstdigitised. Information concerning each channel is then transmitted sequentiallyrather than simultaneously, with each link occupying successive time "slots".

3. Standards for digital communicationsevolved separately within Europe and North America. In the United States,the then dominant public network carrier (the Bell system, run by AT&T)established digital data standards. The basic building block, a T-1 link,carries the equivalent of 24 telephone channels at a rate of 1.544 Mbps.Higher capacity systems operate at greater data transmission rates Thus,the highest transmission rate, T-5, carries the equivalent of 8,000 speechchannels at a data rate of 560 Mbps.

4. Europe adopted a different frameworkfor digital communications, based on standards originally agreed by theCEPT. The basic European standard digital link, E-1, carries 30 telephonechannels at a data rate of 2 Mbps. Most European telecommunications systemsare based on E-1 links or (as in North America), multiples thereof. Thedistinction is significant because most Comint processing equipment manufacturedin the United States is designed to handle intercepted communications workingto the European forms of digital communications.

5. Recent digital systems utilise synchronisedsignals carried by very high capacity optical fibres. Synchronising signalsenables single channels to be easily extracted from high capacity links.The new system is known in the US as the synchronous optical network (SONET),although three equivalent definitions and labels are in use.(75)

Communications intelligenceequipment

6. Dozens of US defence contractors, manylocated in Silicon Valley (California) or in the Maryland "Beltway" areanear Washington, manufacture sophisticated Sigint equipment for NSA. MajorUS corporations, such as Lockheed Martin, Space Systems/Loral, TRW, Raytheonand Bendix are also contracted by NSA to operate major Sigint collectionsites. A full report on their products and services is beyond the scopeof this study. The state of the art in contemporary communications intelligencemay usefully be demonstrated, however, by examining some of the Comintprocessing products of two specialist NSA niche suppliers: Applied SignalTechnology Inc (AST), of Sunnyvale, California, and The IDEAS Operationof Columbia, Maryland (part of Science Applications International Corporation(SAIC)).(76)

7. Both companies include senior ex-NSAstaff as directors. When not explicitly stated, their products can be identifiedas intended for Sigint by virtue of being "TEMPEST screened". AST statesgenerally that its "equipment is used for signal reconnaissance of foreigntelecommunications by the United States government". One leading cryptographerhas aptly and and engagingly described AST as a "one-stop ECHELON shop".

Widebandextraction and signal analysis

8. Wideband (or broadband) signals arenormally intercepted from satellites or tapped cables in the form of multiplexmicrowave or high frequency signals. The first step in processing suchsignals for Comint purposes is "wideband extraction". An extensive rangeof Sigint equipment is manufactured for this purpose, enabling newly interceptedsystems to be surveyed and analysed. These include transponder survey equipmentwhich identify and classify satellite downlinks, demodulators, decoders,demultiplexers, microwave radio link analysers, link survey units, carrieranalysis systems, and many other forms of hardware and software.

9. A newly intercepted communicationssatellite or data link can be analysed using the AST Model 196

9. A newly intercepted communicationssatellite or data link can be analysed using the AST Model 196 "Transpondercharacterisation system". Once its basic communications structure has beenanalysed, the Model 195 "Wideband snapshot analyser", also known as SNAPPER,can record sample data from even the highest capacity systems, sufficientto analyse communications in minute detail. By the start of 1999, operatingin conjunction with the Model 990 "Flexible Data Acquisition Unit", thissystems was able to record, playback and analyse at data rates up to 2.488Gbps (SONET OC-48). This is 16 times faster than the largest backbone linksin general use on the Internet; larger than the telephony capacity of anycurrent communications satellite; and equivalent to 40,000 simultaneoustelephone calls. It can be fitted with 48 Gbyte of memory (500-1000 timeslarger than found in an average personal computer), enabling relativelylengthy recordings of high-speed data links. The 2.5 Gbps capacity of asingle SNAPPER unit exceeds the current daily maximum data rate found ona typical large Internet exchange.(77)

10. Both AST and IDEAS offer a widerange of recorders, demultiplexers, scanners and processors, mostly designedto process European type (CEPT) E-1, E-3 (etc) signals at data rates ofup to 160 Mbps. Signals may be recorded to banks of high-speed tape recorders,or into high capacity "RAID"(78)hard disk networks. Intercepted optical signals can be examined with theAST Model 257E "SONET analyser".

11. Once communications links havebeen analysed and broken down to their constituent parts, the next stageof Comint collection involves multi-channel processors which extract andfilter messages and signals from the desired channels. There are threebroad categories of interest: "voice grade channels", normally carryingtelephony; fax communications; and analogue data modems. A wide selectionof multi-channel Comint processors are available. Almost all of them separatevoice, fax and data messages into distinct "streams" for downstream processingand analysis.

12. The AST Model 120 multi-channelprocessor - used by NSA in different configurations known as STARQUAKE,COBRA and COPPERHEAD - can handle 1,000 simultaneous voice channels andautomatically extract fax, data and voice traffic. Model 128, larger still,can process 16 European E-3 channels (a data rate of 500 Mbps) and extract480 channels of interest. The 1999 giant of AST's range, the Model 132"Voice Channel Demultiplexer", can scan up to 56,700 communications channels,extracting more than 3,000 voice channels of interest. AST also providesSigint equipment to intercept low capacity VSAT(79)satellite services used by smaller businesses and domestic users. Thesesystems can be intercepted by the AST Model 285 SCPS processor, which identifiesand extracts up to 48 channels of interest, distinguished between voice,fax and data.

13. According to US government publications,an early Wideband Extraction system was installed at NSA's Vint Hill Farmsfield station in 1970, about the time that systematic COMSAT interceptioncollection began. That station is now closed. US publications identifythe NSA/CSS Regional Sigint Operations Centre at San Antonio, Texas, asa site currently providing a multi-channel Wideband Extraction service.

Filtering,data processing, and facsimile analysis

14. Once communications channels havebeen identified and signals of interest extracted, they are analysed furtherby sophisticated workstations using special purpose software. AST's ELVIRASignals Analysis Workstation is typical of this type of Sigint equipment.This system, which can be used on a laptop computer in covert locations,surveys incoming channels and extracts standard Comint data, includingtechnical specifications (STRUM) and information about call destinations(SRI, or signal related information). Selected communications are relayedto distant locations using NSA standard "Collected Signals Data Format"(CSDF).(80)

15. High-speed data systems can alsobe passed to AST's TRAILMAPPER software system, which works at a data rateof up to 2.5 Gbps. It can interpret and analyse every type of telecommunicationssystem, including European, American and optical standards. TRAILMAPPERappears to have been designed with a view to analysing ATM (asynchronoustransfer mode) communications. ATM is a modern, high-capacity digital communicationssystem. It is better suited than standard Internet connections to carryingmultimedia traffic and to providing business with private networks (VPN,LAN or WAN). TRAILMAPPER will identify and characterise such business networks.

16. In the next stage downstream, interceptedsignals are processed according to whether they are voice, fax or data.AST's "Data Workstation" is designed to categorise all aspects of datacommunications, including systems for handling e-mail or sending fileson the Internet.(81)Although the very latest modem systems (other than ISDN) are not includedin its advertised specification, it is clear from published research thatAST has developed the technology to intercept and process the latest datacommunications systems used by individuals and business to access the Internet.(82)The Data Workstation can stored and automatically process 10,000 differentrecorded signals.

17. Fax messages are processed by AST'sFax Image Workstation. This is described as a "user friendly, interactiveanalysis tool for rapid examination images stored on disk. Although notmentioned in AST's literature, standard fax pre-processing for Dictionarycomputers involves automatic "optical character recognition" (OCR) software.This turns the typescript into computer readable (and processable)

text.The effectiveness of these systemsmakes fax-derived Comint an important collection subsystem. It has onedrawback. OCR computer systems that can reliably recognise handwritingdo not exist. No one knows how to design such a system. It follows that,perversely, hand-written fax messages may be a secure form of communicationthat can evade Dictionary surveillance criteria, provided always that theassociated "signal related information" (calling and receiving fax numbers)have not been recognised as being of interest and directed to a Fax ImageWorkstation.

18. AST also make a "Pager Identificationand Message Extraction" system which automatically collects and processesdata from commercial paging systems. IDEAS offer a Video TeleconferencingProcessor that can simultaneously view or record two simultaneous teleconferencingsessions. Sigint systems to intercept cellular mobile phone networks suchas GSM are not advertised by AST or IDEAS, but are available from otherUS contractors. The specifications and ready availability of such systemsindicate how industrialised and pervasive Comint has became. It has movedfar from the era when (albeit erroneously), it was publicly associatedonly with monitoring diplomatic or military messages.
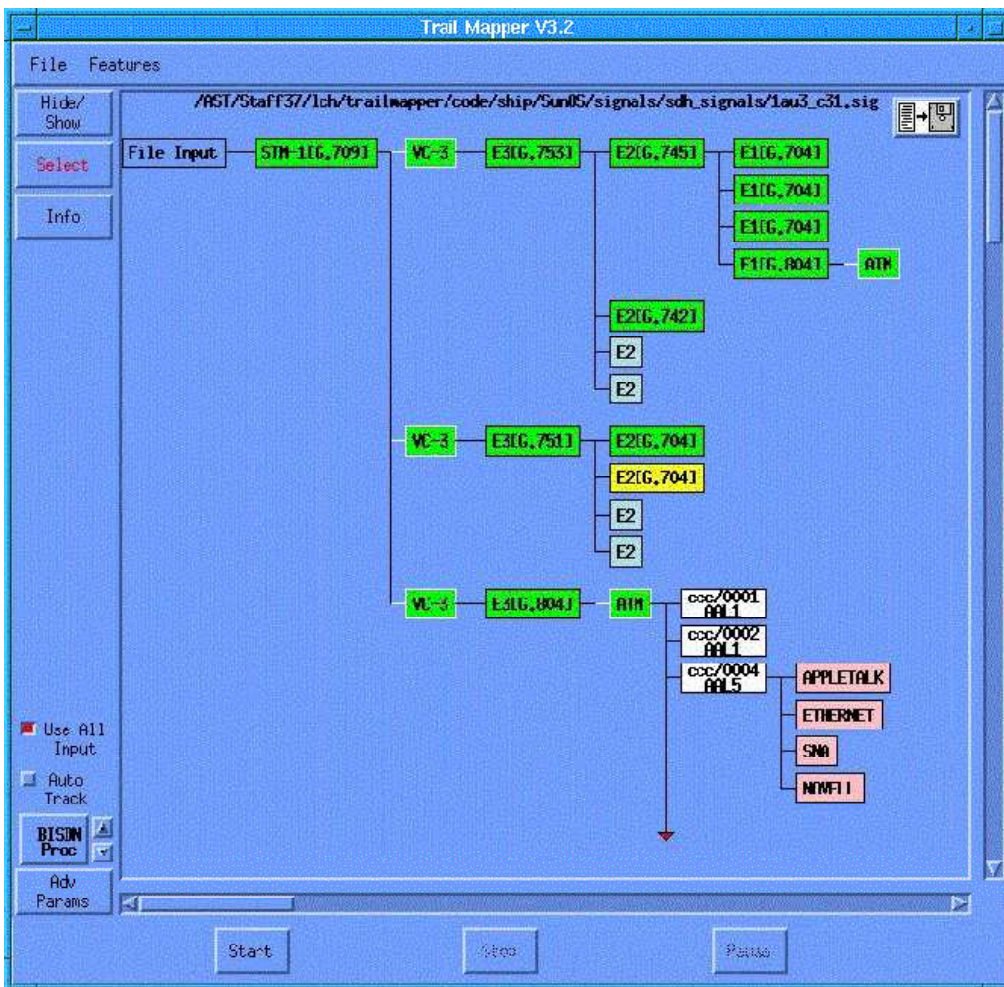
NSA "Trailmapper software showing atomatic detection of private networks inside intercepted high capacity STM-1 digital communications system

Traffic analysis, keyword recognition, text retrieval, and topic analysis

19. Traffic analysis is a method of obtaining intelligence from signal related information, such as the number dialled on a telephone call, or the Calling Line Identification Data (CLID) which identifies the person making the call. Traffic analysis can be used where message content is not available, for example when encryption is used. By analysing calling patterns, networks of personal associations may be analysed and studied. This is a principal method of examining voice communications.

20. Whenever machine readable communications are available, keyword recognition is fundamental to Dictionary computers, and to the ECHELON system. The Dictionary function is straightforward. Its basic mode of operation is akin to web search engines. The differences are of substance and of scale. Dictionaries implement the tasking of their host station against the entire mass of collected communications, and automate the distribution of selected raw product.

21. Advanced systems have been developed to perform very high speed sorting of large volumes of intercepted information. In the late 1980s, the manufacturers of the RHYOLITE Sigint satellites, TRW, designed and manufactured a Fast Data Finder (FDF) microchip for NSA. The FDF chip was declassified in 1972 and made available for commercial use by a spin-off company, Paracel. Since then Paracel has sold over 150 information filtering systems, many of them to the US government. Paracel describes its current FDF technology as the "fastest, most accurate adaptive filtering system in the world":

> A single TextFinder application may involve trillions of bytes of textual archive and thousands of online users, or gigabytes of live data stream per day that are filtered against tens of thousands of complex interest profiles ... the TextFinder chip implements the most comprehensive character-string comparison functions of any text retrieval system in the world.

Devices like this are ideal for use in ECHELON and the Dictionary system.

22. A lower capacity system, the PRP-9800 Pattern Recognition Processor, is manufactured by IDEAS. This is a computer card which can be fitted to a standard PC. It can analyse data streams at up to 34 Mbps (the European E-3 standard), matching every single bit to more than 1000 pre-selected patterns.

23. Powerful though Dictionary methods and keyword search engines may be, however, they and their giant associated intelligence databases may soon seem archaic. Topic analysis is a more powerful and intuitive technique, and one that NSA is developing and promoting with confidence. Topic analysis enables Comint customers to ask their computers to "find me documents about subject X". X might be "Shakespeare in love" or "Arms to Iran".

24. In a standard US test used to evaluate topic analysis systems, (83) one task the analysis program is given is to find information about "Airbus subsidies". The traditional approach involves supplying the computer with the key terms, other relevant data, and synonyms. In this example, the designations A-300 or A-320 might be synonymous with "Airbus". The disadvantage of this approach is that it may find irrelevant intelligence (for example, reports about export subsidies to goods flown on an Airbus) and miss relevant material (for example a financial analysis of a company in the consortium which does not mention the Airbus product by name). Topic analysis overcomes this and is better matched to human intelligence.

25. The main detectable thrust of NSA research on topic analysis centres on a method called N-gram analysis. Developed inside NSA's Research group - responsible for Sigint automation- N-gram analysis is a fast, general method of sorting and retrieving machine-readable text according to language and/or topic. The N-gram system is claimed to work independently of the language used or the topic studied. NSA patented the method in 1995. (84)

26. To use N-gram analysis, the operator ignores keywords and defines the enquiry by providing the system with selected written documents concerning the topic of interest. The system determines what the topic is from the seed group of documents, and then calculates the probability that other documents cover the same topic. In 1994, NSA made its N-gram system available for commercial exploitation. NSA's research group claimed that it could be used on "very large data sets (millions of documents)", could be quickly implemented on any computer system and that it could operate effectively "in text containing a great many errors (typically 10-15% of all characters)".

27. According to former NSA Director William Studeman, "information management will be the single most important problem for the (US) Intelligence Community" in the future. (85) Explaining this point in 1992, he described the type of filtering involved in systems like ECHELON:

> One [unidentified] intelligence collection system alone can generate a million inputs per half hour; filters throw away all but 6500 inputs; only 1,000 inputs meet forwarding criteria; 10 inputs are normally selected by analysts and only one report is produced. These are routine statistics for a number of intelligence collection and analysis systems which collect technical intelligence.
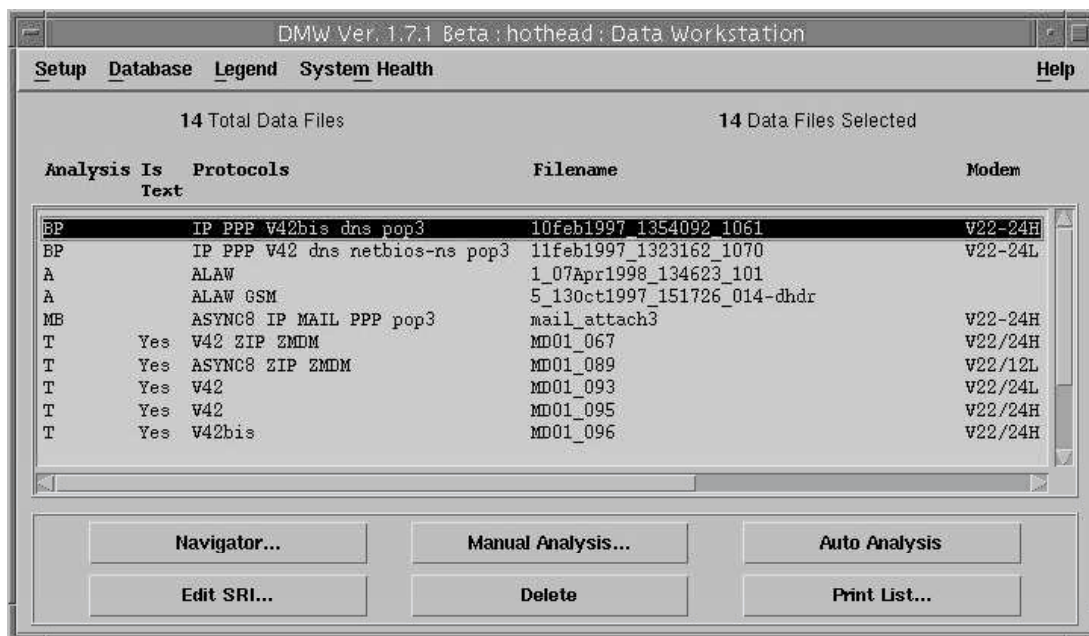
The "Data Workstation" Comint software system analyses up to 10,000 recorded messages, identifying Internet traffic, e-mail messages and attachments

Speech recognition systems

28. For more than 40 years, NSA, ARPA, GCHQ and the British government Joint Speech Research Unit have conducted and sponsored research into speech recognition. Many press reports (and the previous STOA report) have suggested that such research has provided systems which can automatically select telephone communications of intelligence interest based on the use of particular "key words" by a speaker. If available, such systems would enable vastly more extensive Comint information to be gathered from telephone conversations than is available from other methods of analysis. The contention that telephone word-spotting systems are readily available appears to by supported by the recent availability of a string of low-cost software products resulting from this research. These products permit PC users to dictate to their computers instead of entering data through the keyboard. (86)

29. The problem is that for Comint applications, unlike personal computer dictation products, speech recognition systems have to operate in a multi-speaker, multi-language environment where numerous previously never heard speakers may each feature physiological differences, dialect variations, and speech traits. Commercial PC systems usually require one or more hours of training in order reliably to recognise a single speaker. Even then, such systems may mistranscribe 10% or more of the words spoken.

30. In PC dictation applications, the speaker can correct mistranscriptions and continually retrain the

30. In PC dictation applications, thespeaker can correct mistranscriptions and continually retrain the recognitionsystem, making a moderate error rate acceptable. For use in Comint, wherethe interception system has no prior knowledge of what has been said (oreven the language in use), and has to operate in the poorer signal environmentof a telephone speech channel, such error rates are unachievable. Worsestill, even moderate error rates can make a keyword recognition systemworthless by generating both false positive outputs (words wrongly identifiedas keywords) and false negative outputs (missing genuine keywords).

31. This study has found no evidencethat voice keyword recognition systems are currently operationally deployed,nor that they are yet sufficiently accurate to be worth using for intelligencepurposes.

Continuousspeech recognition

32. The fundamental technique in manyspeech recognition applications is a statistical method called Hidden MarkovModelling (HMM). HMM systems have been developed at many centres and areclaimed academically to offer "good word spotting performance ... usingvery little or no acoustic speech training".(87)The team which reported this result tested its system using data from theUS Department of Defense "Switchboard Data", containing recordings of thousandof different US telephone conversations. On a limited test the probabilitiesof correctly detecting the occurrences of 22 keywords ranged from 45-68%on settings which allowed for 10 false positive results per keyword perhour. Thus if 1000 genuine keywords appeared during an hour's conversation,there would be at least 300 missed key words, plus 220 false alarms.

33. At about the same time, (February1990), the Canadian Sigint organisation CSE awarded a Montreal-based computerresearch consultancy the first of a series of contracts to develop a Comintwordspotting system.(88)The goal of the project was to build a word-spotter that worked well evenfor noisy calls. Three years later, CRIM reported that "our experiencehas taught us that, regardless of the environmental conditions, wordspottingremains a difficult problem". The key problem, which is familiar to humanlisteners, is that a single word heard on its own can easily be misinterpreted,whereas in continuous speech the meaning may be deduced from surroundingwords. CRIM concluded in 1993 that "it is probable that the most effectiveway of building a reliable wordspotter is to build a large vocabulary continuousspeech recognition (CSR) system".

34. Continuous speech recognition softwareworking in real time needs a powerful fast, processor. Because of the lackof training and the complex signal environment found in intercepted telephonecalls, it is likely that even faster processors and better software thanused in modern PCs would yield poorer results than are now provided bywell-trained commercial systems. Significantly, an underlying problem isthat voice keyword recognition is, as with machine-readable messages, animperfect means to the more useful intelligence goal - topic spotting.

35. In 1993, having failed to builda workable wordspotter, CRIM suggesting "bypassing" the problem and attemptinginstead to develop a voice topic spotter. CRIM reported that "preliminaryexperiments reported at a recent meeting of American defense contractors... indicate that this may in fact be an excellent approach to the problem".They offered to produce an "operational topic spotting" system by 1995.They did not succeed. Four years later, they were still experimenting onhow to built a voice topic spotter.(89)They received a further research contract. One method CRIM proposed wasNSA's N-gram technique.

Speakeridentification and other voice message selection techniques

36. In 1993, CRIM also undertook to supplyCSE with an operational speaker identification module by March 1995. Nothingmore was said about this project, suggesting that the target may have beenmet. In the same year, according to NSA documents, the IDEAS company supplieda "Voice Activity Detector and Analyser", Model TE464375-1, to NSA's officesinside GCHQ Cheltenham. The unit formed the centre of a 14-position computerdriven voice monitoring system. This too may have been an early speakeridentification system.

37. In 1995, widely quoted reportssuggested that NSA speaker identification had been used to help capturethe drug cartel leader Pablo Escobar. The reports bore strong resemblanceto a novel by Tom Clancy, suggesting that the story may have owed moreto Hollywood than high tech. In 1997, the Canadian CRE awarded a contractto another researcher to develop "new retrieval algorithms for speech characteristicsused for speaker identification", suggesting this method was not by thena fully mature technology. According to Sigint staff familiar with thecurrent use of Dictionary, it can be programmed to search to identify particularspeakers on telephone channels. But speaker identification is still nota particularly reliablr or effective Comint technique.(90)

38. In the absence of effective wordspottingor speaker identification techniques, NSA has sought alternative meansof automatically analysing telephone communications. According NSA's classificationguide, other techniques examined include Speech detection - detecting thepresence or absence of speech activity; Speaker discrimination - techniquesto distinguish between the speech of two or more speakers; and Readabilityestimation - techniques to determine the quality of speech signals. Systemdescriptions must be classified "secret" if NSA "determines that they representmajor advances over techniques known in the research community".(91)

"Workfactor reduction"; thesubversion of cryptographic systems

39. From the 1940s to date, NSA has underminedthe effectiveness of cryptographic systems made or used in Europe. Themost important target of NSA activity was a prominent Swiss manufacturingcompany, Crypto AG. Crypto AG established a strong position as a supplierof code and cypher systems after the second world war. Many governmentswould not trust products offered for sale by major powers. In contrast,Swiss companies in this sector benefited from Switzerland's neutralityand image of integrity.

40. NSA arranged to rig encryptionsystems sold by Crypto AG, enabling UKUSA agencies to read the coded diplomaticand military traffic of more than 130 countries. NSA's covert interventionwas

arranged through the company's owner and founder Boris Hagelin, andinvolved periodic visits to

arranged through the company's owner and founder Boris Hagelin, andinvolved periodic visits to Switzerland by US "consultants" working forNSA. One was Nora L MacKabee, a career NSA employee. A US newspaper obtainedcopies of confidential Crypto AG documents recording Ms Mackebee's attendanceat discussion meetings in 1975 to design a new Crypto AG machine".(92)

41. The purpose of NSA's interventionswere to ensure that while its coding systems should appear secure to othercryptologists, it was not secure. Each time a machine was used, its userswould select a long numerical key, changed periodically. Naturally userswished to selected their own keys, unknown to NSA. If Crypto AG's machineswere to appear strong to outside testers, then its coding system shouldwork, and actually be strong. NSA's solution to this apparent condundrumwas to design the machine so that it broadcast the key it was using tolisteners. To prevent other listeners recognising what was happening, thekey too had also to be sent in code - a different code, known only to NSA.Thus, every time NSA or GCHQ intercepted a message sent using these machines,they would first read their own coded part of the message, called the "hilfsinformationen"(help information field) and extract the key the target was using. Theycould then read the message itself as fast or even faster than the intendedrecipient(93)

42. The same technique was re-usedin 1995, when NSA became concerned about cryptographic security systemsbeing built into Internet and E-mail software by Microsoft, Netscape andLotus. The companies agreed to adapt their software to reduce the levelof security provided to users outside the United States. In the case ofLotus Notes, which includes a secure e-mail system, the built-in cryptographicsystem uses a 64 bit encryption key. This provides a medium level of security,which might at present only be broken by NSA in months or years.

43. Lotus built in an NSA "help information"trapdoor to its Notes system, as the Swedish government discovered to itsembarrassment in 1997. By then, the system was in daily use for confidentialmail by Swedish MPs, 15,000 tax agency staff and 400,000 to 500,000 citizens.Lotus Notes incorporates a "workfactor reduction field" (WRF) into alle-mails sent by non US users of the system. Like its predecessor the CryptoAG "help information field" this device reduces NSA's difficulty in readingEuropean and other e-mail from an almost intractable problem to a few secondswork. The WRF broadcasts 24 of the 64 bits of the key used for each communication.The WRF is encoded, using a "public key" system which can only be readby NSA. Lotus, a subsidiary of IBM, admits this. The company told SvenskaDagbladet:

> "The difference between the AmericanNotes version and the export version lies in degrees of encryption. Wedeliver 64 bit keys to all customers, but 24 bits of those in the versionthat we deliver outside of the United States are deposited with the Americangovernment".(94)

44. Similar arrangements are built intoall export versions of the web "browsers" manufactured by Microsoft andNetscape. Each uses a standard 128 bit key. In the export version, thiskey is not reduced in length. Instead, 88 bits of the key are broadcastwith each message; 40 bits remain secret. It follows that almost everycomputer in Europe has, as a built-in standard feature, an NSA workfactorreduction system to enable NSA (alone) to break the user's code and readsecure messages.

45. The use of powerful and effectiveencryption systems will increasingly restrict the ability of Comint agenciesto process collected intelligence. "Moore's law" asserts that the costof computational power halves every 18 months. This affects both the agenciesand their targets. Cheap PCs can now efficiently perform complex mathematicalcalculations need for effective cryptography. In the absence of new discoveriesin physics or mathematics Moore's law favours codemakers, not codebreakers.

Illustrations : D Campbell; US AirForce; IPTV Ltd; Stephen King; Charles V Pick; IPTV Ltd; Jim Bamford, GCHQ; US Navy; KGB/RussianSecurity Service; D Campbell.

Glossary and definitions

ATM	AsynchronousTransfer Mode; a high speed form of digital communications increasinglyused for on the Internet
BND	Bundesachrichtendienst;the foreign intelligence agency of the Federal Republic of Germany. Itsfunctions include Sigint
CCITT	ConsultativeCommittee for International Telephony and Telegraphy; United Nations agencydeveloping standards and protocols for telecommunications; part of theITU; also known as ITU-T
CEPT	ConferenceEuropeene des Postes et des Telecommunications
CLID	Calling LineIdentification Data
Comint	Comint CommunicationsIntelligence
COMSAT	(Civil or commercial)communications satellite; for military communications usage, the phraseologyis commonly reversed, i.e., SATCOM.
CRIM	CRIM Centrede Recherche Informatique de Montreal
CSDF	CSDF CollectedSignals Data Format; a term used only in Sigint
CSE	CSE CommunicationsSecurity Establishment, the Sigint agency of Canada
CSS	CSS CentralSecurity Service; the military component of NSA
DARPA	DARPA DefenseAdvanced Research Projects Agency (United States Department of Defense)
DGSE	DirectorateGeneral de Securite Exteriere, the foreign intelligence agency of France.Its functions include Sigint

DSD	DSD DefenceSignals Directorate, the Sigint agency of the Commonwealth of Australia
DODJOCC	DODJOCC Departmentof Defense Joint Operations Centre Chicksands
E1, E3 (etc)	Standard fordigital or TDM communications systems defined by the CEPT, and primarilyused within Europe and outside North America
ENFOPOL	EU designationfor documents concerned with law enforcement matters/police
FAPSI	FederalnoeAgenstvo Pravitelstvennoi Svyazi i Informatsii, the Federal Agency forGovernment Communications and Information of Russia. Its functions includeSigint
FBI	FBI FederalBureau of Investigation; the national law enforcement and counter-intelligenceagency of the United States
FDF	FDF Fast DataFinder
FDM	FDM FrequencyDivision Multiplex; a form of multi-channel communications based on analoguesignals
FISA	FISA ForeignIntelligence Surveillance Act (United States)
FISINT	FISINT ForeignInstrumentation Signals Intelligence, the third branch of Sigint
Gbps	Gigabits persecond
GCHQ	GCHQ GovernmentCommunications Headquarters; the Sigint agency of the United Kingdom
GHz	GigaHertz
Gisting	Within Sigint,the analytical task of replacing a verbatim text with the sense or mainpoints of a communication
HDLC	HDLC High-levelData Link Control
HF	HF High Frequency;frequencies from 3MHz to 30MHz
HMM	HMM HiddenMarkov Modelling, a technique widely used in speech recognition systems.
ILETS	ILETS InternationalLaw Enforcement Telecommunications Seminar
Intelsat	InternationalTelecommunications Satellite
IOSA	IOSA InterimOverhead Sigint Architecture
Iridium	Satellite PersonalCommunications System involving 66 satellites in low earth orbit, providingglobal communications from mobile telephones
ISDN	ISDN IntegratedServices Data Network
ISP	ISP InternetService Provider
ITU	ITU InternationalTelecommunications Union
IUR	IUR InternationalUser Requirements (for communications interception); IUR 1.0 was preparedby ILETS (qv) in 1994
IXP	IXP InternetExchange Point
LAN	LAN Local AreaNetwork
LES	LEA Law EnforcementAgency (American usage)
Mbps	Megabits persecond
MHz	MegaHertz
Microwave	Radio signalswith wavelengths of 10cm or shorter; frequencies above 1GHz
Modem	Modem Devicefor sending data to and from (e.g.) a computer; a "modulator-demodulator)
MIME	MIME MultipurposeInternet Message Extension; a systems used for sending computer files,images, documents and programs as "attachments" to an e-mail message
N-gramanalysis	A system foranalysing textual documents; in this context, a system for matching a largegroup of documents to a smaller group embodying a topic of interest. Themethod depends on counting the frequency with which character groups oflength N appear in each document; hence N-gram
NSA	NSA NationalSecurity Agency, the Sigint agency of the United States
OCR	Optical CharacterRecognition
PC	Personal Computer
PCS	Personal CommunicationsSystems; the term includes mobile telephone systems, paging systems andfuture wide area radio data links for personal computers, etc
POP/POP3	Post OfficeProgram; a system used for receiving and holding e-mail
PTT	Posts Telegraphand Telephone (Administration or Authority)

RAID	Redundant Array of Inexpensive Disks
SCI	Sensitive Compartmented Intelligence; used to limit access to Comint information according to "compartments"
SCPC	Single Channel Per Carrier; low capacity satellite communications system
SMTP	Standard Mail Transport Protocol
Sigint	Signals Intelligence
SONET	Synchronous Optical Network
SMDS	Switched Multi-Megabit Data Service
SMO	Support for Military Operations
SPCS	Satellite Personal Communications Systems
SRI	Signal Related Information; a term used only in Sigint
STOA	Science and Technology Assessments Office of the European Parliament; the body commissioning this report
T1,T3 (etc)	Digital or TDM communications systems originally defined by the Bell telephone system in North America, and primarily used there
TCP/IP	Terminal Control Protocol/Internet Protocol
TDM	Time Division Muliplex; a form of multi-channel communications normally based on digital signals
Traffic analysis	Within Sigint, a method of analysing and obtaining intelligence from messages without reference to their content; for example by studying the origin and destination of messages with a view to eliciting the relationship between sender and recipient, or groups thereof
UKUSA	UK-USA agreement
VPN	Virtual Private Network
VSAT	Very Small Aperture Terminal; low capacity satellite communications system serving home and business users
WAN	Wide Area Network
WRF	Workfactor Reduction Field
WWW	World Wide Web
	X.25, V.21, V.34, V.90, V.100 (etc) are CCITT telecommunications standards

Notes

1. UKUSA refers to the 1947 United Kingdom - United States agreement on Signals intelligence. The nations of the UKUSA alliance are the United States (the "First Party"), United Kingdom, Canada, Australia and New Zealand (the "Second Parties").

2. "An appraisal of the Technologies of Political Control", Steve Wright, Omega Foundation, European Parliament (STOA), 6 January 1998.

3. "They've got it taped", Duncan Campbell, New Statesman, 12 August 1988. "Secret Power : New Zealand's Role in the International Spy Network", Nicky Hager, Craig Potton Publishing, PO Box 555, Nelson, New Zealand, 1996.

4. National Security Council Intelligence Directive No 6, National Security Council of the United States, 17 February 1972 (first issued in 1952).

5. SIGINT is currently defined as consisting of COMINT, ELINT (electronic or non-communications intelligence and FISINT (Foreign Instrumentation Signals Intelligence).

6. Statement by Martin Brady, Director of DSD, 16 March 1999. To be broadcast on the Sunday Programme, Channel 9 TV (Australia), May 1999.

7. "Farewell", despatch to all NSA staff, William Studeman, 8 April 1992. The two business areas to which Studeman referred were "increased global access" and "SMO" (support to military operations).

8. *Federalnoe Agenstvo Pravitelstvennoi Svyazi i Informatsii*, the (Russian) Federal Agency for Government Communications and Information. FAPSI's functions extend beyond Comint and include providing government and commercial communications systems.

9. Private communications from former NSA and GCHQ employees.

10. Sensitive Compartmented Intelligence.

11. See note 1.

12. Private communications from former GCHQ employees; the US Act is the Foreign Intelligence Surveillance Act (FISA).

13. See note 6.

14. In 1919, US commercial cable companies attempted to resist British government demands for

14.In 1919, US commercial cable companies attempted to resist British governmentdemands for access to all cables sent overseas. Three cable companies testifiedto the US Senate about these practices in December 1920. In the same year,the British Government introduced legislation (the Official Secrets Act,1920, section 4) providing access to all or any specified class of communications.The same power was recodified in 1985, providing lawful access for Comintpurposes to all "external communications", defines as any communicationswhich are sent from or received outside the UK (Interception of CommunicationAct 1984, Section 3(2)). Similar requirements on telecommunications operatorsare made in the laws of the other UKUSA countries. See also "OperationSHAMROCK", (section 3).

15."ThePuzzle Palace", James Bamford, Houghton Mifflin, Boston, 1982, p331.

16.Personalcommunications from former NSA and GCHQ employees.

17."Dispatches: The Hill", transmitted by Channel 4 Television (UK), 6 October 1993.DODJOCC stood for Department of Defense Joint Operations Centre Chicksands.

18."TheJustice Game", Geoffrey Robertson, Chapter 5, Chatto and Windus, London,1998

19.Finkreport to the House Committee on Government Operations, 1975, quoted in"NSA spies on the British government", New Statesman, 25 July 1980

20."Amerikanskiyesputniki radioelektronnoy razvedki na Geosynchronnykh orbitakh" ("AmericanGeosynchronous SIGINT Satellites"), Major A Andronov, Zarubezhnoye VoyennoyeObozreniye, No.12, 1993, pps 37-43.

21."Spacecollection", in The US Intelligence Community (fourth edition), JeffreyRichelson, Westview, Boulder, Colorado, 1999, pages 185-191.

22.Seenote 18.

23.Richelson,op cit.

24."UKEyes Alpha", Mark Urban, Faber and Faber, London, 1996, pps 56-65.

25.Besidesthe stations mentioned, a major ground station whose targets formerly includedSoviet COMSATs is at Misawa, Japan. Smaller ground stations are locatedat Cheltenham, England; Shoal Bay, Australia.

26."Swordand Shield : The Soviet Intelligence and Security Apparatus", Jeffrey Richelson,Ballinger, Cambridge, Massachusetts, 1986.

27."LesFrancais aussi ecountent leurs allies", Jean Guisnel, Le Point, 6 June1998.

28.Intelligence(Paris), 93, 15 February 1999, p3.

29."Blindmans Bluff : the untold story of American submarine espionage", SherrySontag and Christopher Drew, Public Affairs, New York, 1998.

30.Ibid.

31.Ibid

32.Aspecimen of the IVY BELLS tapping equipment is held in the former KGB museumin Moscow. It was used on a cable running from Moscow to a nearby scientificand technical institution.

33.TCP/IP.TCP/IP stands for Terminal Control Protocol/Internet Protocol. IP is thebasic network layer of the Internet.

34.GCHQwebsite at http://www.gchq.gov.uk/technol.html

35.Personalcommunication from DERA. A Terabyte is one thousand Gigabytes, i.e., 1012bytes.

36.Personalcommunication from John Young.

37."Puzzlepalace conducting internet surveillance", Wayne Madsen, Computer Fraudand Security Bulletin, June 1995.

38.Ibid.

39."MoreNaked Gun than Top Gun", Duncan Campbell, Guardian, 26 November 1997.

40."Spyworld",Mike Frost and Michel Gratton, Doubleday Canada, Toronto, 1994.

41.TheNational Security Agency and Fourth Amendment Rights, Hearings before theSelect Committee to Study Government Operations with Respect to IntelligenceActivitities, US Senate, Washington, 1976.

42.Letterfrom, Lt Gen Lew Allen, Director of NSA to US Attorney General Elliot Richardson,4 October 1973; contained in the previous document.

43.Privatecommunication.

44.Worldin Action, Granada TV.

45.Thisarrangements appears to be an attempt to comply with legal restrictionsin the Interception of Communications Act 1985, which prohibit GCHQ fromhandling messages except those identified in government "certificates"which "describe the intercepted material which should be examined". TheAct specifies that "so much of the intercepted material as is not certifiedby the certificate is not [to be] read, looked at or listened to by anyperson". It appears from this that, although all messages passing throughthe United Kingdom are intercepted and sent to GCHQ's London office, theorganisation considers that by having British Telecom staff operate theDictionary computer, it is still under the control of the telecommunicationsnetwork operator unless and until it is selected by the Dictionary andpasses from BT to GCHQ.

46. Private communications.

47. "Naval Security Group Detachment, Sugar Grove History for 1990", US Navy, 1 April 1991.

48. Missions, functions and tasks of Naval Security Group Activity (NAVSECGRUACT) Sugar Grove, West Virginia", NAVSECGRU INSTRUCTION C5450.48A, 3 September 1991.

49. Report on tasks of Detachment 3 , 544 Air Intelligence Group, Air Intelligence Agency Almanac, US Air Force, 1998-99.

50. Ibid, Detachment 2, 544 Air Intelligence Group.

51. Information obtained by Bill Robinson, Conrad Grebel College, Waterloo, Ontario. CDF and CFS documents were obtained under the Freedom of Information Act, or published on the World Wide Web.

52. Career resume of Patrick D Duguay, published at: http://home.istar.ca/~pdduguay/resume.htm

53. CSE Financial Status Report, 1 March 1996, released under the Freedom of Information Act. Further details about "ECHELON" were not provided. It is therefore ambiguous as to whether the expenditure was intended for the ECHELON computer system, or for different functions (for example telecommunications or power services).

54. "Secret Power", op cit.

55. Twenty/Twenty, TV3 (New Zealand), October 1999.

56. Interview with David Herson, Head of Senior Officers' Group on Information Security, EU, by staff of Engineering Weekly (Denmark), 25 September 1996. Published at http://www.inq.dk/arkiv/herson.htm

57. Council Resolution on the Lawful Interception of Telecommunications, 17 January 1995, (96 C_329/01)

58. "International Harmonisation of Technical Requirements for Legal Interception of Telecommunications", Resolution 1115, Tenth Plenary meeting of the ITU Council, Geneva, 27 June 1997.

59. ENFOPOL 98, Draft Resolution of the Council on Telecommunications Interception in respect of New Technology. Submitted by the Austrian Presidency. Brussels, 3 September 1998.

60. ENFOPOL 19, 13 March 1999.

61. European Parliament, 14 September 1998.

62. "Uncle Sam's Eavesdroppers", Close Up North, BBC North, 3 December 1998; reported in "Star Wars strikes back", Guardian, 3 December 1998

63. "Dispatches: The Hill", Channel 4 Television (UK), 6 October 1993

64. Ibid.

65. "Mixing business with spying; secret information is passed routinely to U.S.", Scott Shane, Baltimore Sun, 1 November 1996.

66. "UK Eyes Alpha", op cit, p235.

67. Private communication.

68. See note 62.

69. Raytheon Corp press release: published at: http://www.raytheon.com/sivam/contract.html

70. "America's Fortress of Spies", Scott Shane and Tom Bowman, Baltimore Sun 3 December 1995.

71. "Company Spies", Robert Dreyfuss, Mother Jones, May/June 1994.

72. Financial Post, Canada, 28 February 1998.

73. European Parliament, 16 September 1998.

74. See note 56.

75. Equivalent communications may be known as Synchronous Transport Module (STM) signals within the Synchronous Digital Hierarchy (ITU standard); Synchronous Transport Signals (STS) within the US SONET system; or as Optical Carrier signals (OC).

76. The information about these Sigint systems has been drawn from open sources (only).

77. In April 199, the peak data rate at MAE West was less than 1.9 Gbps.

78. Redundant Arrays of Inexpensive Disks.

79. Very Small Aperture Terminal; SCPC is Single Channel Per Carrier.

80. "Collected Signals Data Format"; defined in US Signals Intelligence Directive 126 and in NSA's CSDF manual. Two associated NSA publications providing further guidance are the Voice Processing Systems Data Element Dictionary and the Facsimile Data Element Dictionary, both issued in March 1997.

81. The Data Workstation processes TCP/IP, PP, SMTP, POP3, MIME, HDLC, X.25, V.100, and modem protocols up to and including V.42 (see glossary).

82. "Practical Blind Demodulators for high-order QAM signals", J R Treichler, M G Larimore and J C Harp, Proc IEEE, 86, 10, 1998, p1907. Mr Treichler is technical director of AST. The paper describes a system used to intercept multiple V.34 signals, extendable to the more recent protocols.

83. The tasks were set in the second Text Retrieval conference (TREC) organised by the ARPA and the US

83. The tasks were set in the second Text Retrieval conference (TREC) organised by the ARPA and the US National Institute of Science and Technology (NIST), Gaithersburg, Maryland. The 7th annual TREC conference took place in Maryland in 1999.

84. "Method of retrieving documents that concern the same topic"; US Patent number 5418951, issued 23 May 1995; inventor, Marc Damashek; rights assigned to NSA.

85. Address to the Symposium on "National Security and National Competitiveness : Open Source Solutions" by Vice Admiral William Studeman, Deputy Director of Central Intelligence and former director of NSA, 1 December 1992, McLean, Virginia.

86. For example, IBM Via Voice, Dragon Naturally Speaking, Lemout and Hauspe VoiceXpress.

87. "A Hidden Markov Model based keyword recognition system", R.C. Rose and D.B. Paul, Proceedings of the International Conference on Accoustics, Speech and Signal processing, April 1990.

88. Centre de Recherche Informatique de Montreal.

89. "Projet detection des Themes", CRIM, 1997; published at http://www.crim.ca/adi/projet2.html.

90. Private communication.

91. NSA/CSS Classification Guide, NSA, revised 1 April 1983.

92. "Rigging the game: Spy Sting", Tom Bowman, Scott Shane, Baltimore Sun, 10 December 1995.

93. "Wer ist der Befugte Vierte?", Der Spiegel, 36, 1996, pp. 206-7.

94. "Secret Swedish E-Mail Can Be Read by the U.S.A", Fredrik Laurin, Calle Froste, Svenska Dagbladet, 18 November 1997.